



UNITED STATES MARINE CORPS

MARINE RESERVE FORCE, FMF, USMCR
4400 DAUPHINE STREET
NEW ORLEANS, LOUISIANA 70146-5400

ForO P5510.1

2

29 JUN 1993

FORCE ORDER P5510.1

From: Commanding General
To: Distribution List

Subj: STANDING OPERATING PROCEDURE FOR THE INFORMATION
SECURITY PROGRAM (SHORT TITLE: SOP FOR ISP)

Ref: (a) OPNAVINST 5510.1

Encl: (1) LOCATOR SHEET

1. Purpose. To publish procedures for the Information Security Program within Marine Reserve Force (MARRESFOR) Headquarters and where applicable for subordinate units.

2. Information

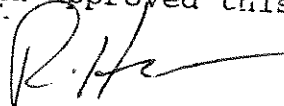
a. The reference supplements and incorporates the policy and guidance set forth in the Department of Defense Information Security Program Regulation (DOD 5200.2) and is the basic directive governing the Information and Personnel Security Program within the Department of the Navy.

b. This Manual implements the applicable provisions of the reference and other pertinent directives as indicated in the body of this Manual.

c. This Manual is applicable to MARRESFOR and the major subordinate commands collocated in New Orleans. Certain provisions of this Manual are applicable to subordinate units geographically separated from this Headquarters.

3. Reserve Applicability. This Manual is applicable to the Marine Corps Reserve.

4. Certification. Reviewed and approved this date.


R. HICKERSON
Chief of Staff

DISTRIBUTION: B

FORO P5510.1

29 JUN 1993

LOCATOR SHEET

Subj: STANDING OPERATING PROCEDURE FOR THE INFORMATION
SECURITY PROGRAM (SHORT TITLE: SOP FOR ISP)

Location:

(Indicate the location(s) of the copy(ies) of this
Manual.)

ENCLOSURE (1)

SOP FOR ISP

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

SOP FOR ISP

CONTENTS

CHAPTER

- 1 BACKGROUND
- 2 PROGRAM MANAGEMENT
- 3 SECURITY EDUCATION
- 4 COMPROMISE AND OTHER SECURITY VIOLATIONS
- 5 MAILING, HANDCARRYING, & TRANSMISSION OF
CLASSIFIED MATERIAL
- 6 ACCOUNTING AND CONTROL
- 7 DESTRUCTION OF CLASSIFIED MATERIAL
- 8 SECURITY & STORAGE OF CLASSIFIED MATERIAL
- 9 REPRODUCTION & PHOTOGRAPHY OF CLASSIFIED MATERIAL
- 10 VISITOR CONTROL & MEETINGS
- 11 PERSONNEL SECURITY INVESTIGATIONS, CLEARANCES,
AND ACCESS PROGRAM
- 12 AUTOMATED DATA PROCESSING SECURITY PROCEDURES

APPENDIX

- A LIST OF REFERENCES

SOP FOR ISP

CHAPTER 1

BACKGROUND -

	PARAGRAPH	PAGE
BASIC GUIDANCE	1000	1-3
AUTHORITY	1001	1-3
APPLICABILITY	1002	1-3
RESPONSIBILITY FOR COMPLIANCE	1003	1-3
ITEMS NOT ADDRESSED	1004	1-4

SOP FOR ISP

CHAPTER 1

BACKGROUND

1000. BASIC GUIDANCE. The Marine Reserve Force (MARRESFOR) Information Security Program (ISP) is established to ensure classified information is protected from unauthorized disclosure and the granting of access to classified information is clearly consistent with the interests of National Security. This Manual supplements applicable portions of the reference for implementation within MARRESFOR, 4th Marine Division, (4th MarDiv), 4th Marine Aircraft Wing (4th MAW), 2d Marine Expeditionary Brigade (2dMEB), 3d Marine Expeditionary Brigade (3dMEB), Marine Corps Reserve Support Command (MCRSC), 4th Force Service Support Group (4th FSSG), and subordinate commands.

1001. AUTHORITY. The Commanding General is responsible for establishing and maintaining an Information and Personnel Security Program per the reference. The MARRESFOR Security Manager is responsible for ensuring that there is an effective program and that it complies with all the directives issued by higher authority. Commanding Generals and Commanding Officers of subordinate units are responsible for establishing and maintaining an Information and Personnel Security Program per the reference and this Manual.

1002. APPLICABILITY

1. This Manual supplements the provisions of the reference and other applicable directives, establishing specific policy and procedures on the handling and security of classified information and material within this Headquarters, 4th MarDiv, 4th MAW, 4th FSSG, and, as applicable, all subordinate units. Information on personnel security provisions published in amplifying or supplemental instructions within this Headquarters will comply with the policies and procedures of higher headquarters directives and this Manual.

2. The term "Supervisor" as used in this Manual refers to the head of organizational sub-entities and includes heads of general and special staff sections, Officers in Charge (OIC) and personnel assigned functional responsibilities for the security of classified material.

1003. RESPONSIBILITY FOR COMPLIANCE

1. The Commanding Officer, Headquarters Battalion, MARRESFOR,

and supervisors are responsible for ensuring compliance with this Manual. They will ensure that all personnel are informed of their responsibilities to safeguard classified information or equipment entrusted to them. They will ensure that only the minimum number of personnel with a need-to-know are authorized clearance and access to classified material.

2. Each individual, military or civilian, assigned to MARRESFOR is responsible for compliance with this Manual in all respects. Any procedure or situation which is a security weakness or could result in an unauthorized disclosure will be immediately reported to the MARRESFOR Security Manager.

1004. ITEMS NOT ADDRESSED. This Manual supplements existing Information and Personnel Security Program directives. It does not fully incorporate all areas of the program. If guidance on a particular matter cannot be found in this Manual or identified references, contact the MARRESFOR Security Manager.

SOP FOR ISP

CHAPTER 2

PROGRAM MANAGEMENT

	PARAGRAPH	PAGE
BASIC POLICY	2000	2-3
DUTIES AND RESPONSIBILITIES	2001	2-3
TURNOVER FILES/DESKTOP PROCEDURES	2002	2-8
INSPECTIONS/INVENTORIES	2003	2-8
TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) . .	2004	2-10
EMERGENCY PLANS	2005	2-10
FORMS	2006	2-10
LETTERS OF APPOINTMENT.	2007	2-10

FIGURES

2-1	ORGANIZATIONAL STRUCTURE	2-12
2-2	FORMAT FOR APPOINTMENT OF SECURITY MANAGER/ASSISTANT SECURITY MANAGER	2-13
2-3	FORMAT FOR APPOINTMENT OF OFFICER IN CHARGE, CLASSIFIED MATERIAL CONTROL CENTER	2-14
2-4	FORMAT FOR APPOINTMENT OF SECONDARY/SUB- CUSTODY CONTROL POINT CUSTODIAN	2-15
2-5	FORMAT FOR APPOINTMENT OF TOP SECRET CONTROL OFFICER	2-16
2-6	FORMAT FOR APPOINTMENT OF COSMIC CONTROL OFFICER	2-17
2-7	FORMAT FOR APPOINTMENT OF TOP SECRET CONTROL ASSISTANT	2-18

SOP FOR ISP

2-8	FORMAT FOR APPOINTMENT OF ADP SECURITY OFFICER . .	2-19
2-9	FORMAT FOR APPOINTMENT OF CMS CUSTODIAN.	2-20

SOP FOR ISP

CHAPTER 2

PROGRAM MANAGEMENT

2000. BASIC POLICY

1. The Commanding General, MARRESFOR is directly responsible for an effective Information and Personnel Security Program. He has delegated the overall coordination of the command security program to the MARRESFOR Security Manager. The organizational structure for accomplishing the management of this program is depicted in Figure 2-1. Responsibilities for various specific areas are further delegated and assigned below. All Supervisors are responsible for compliance with and implementation of the Department of the Navy Information and Personnel Security Program and this Manual within their sections.

2. All Major Subordinate Commands (MSC's), any of their subordinate units (that hold classified material), and MARRESFOR Headquarters Battalion will appoint a Security Manager in writing. The Security Manager must be an officer or civilian employee (GS-11 or above), and have the staff, budget and capability to perform the duties and responsibilities as outlined in the reference and this Manual. All subordinate command Security Managers must have a current (no more than five years old) Special Scope Background Investigation (SSBI). If an SSBI is outdated or nonexistent, then the command will complete the appropriate forms using the reference as a guide and mail it directly to the Defense Investigative Service (DIS).

3. If an Assistant Security Manager is appointed, that person must be a Staff NCO or a GS-5 or above (if a civilian employee) and must have a current favorably adjudicated SSBI. Security Assistants if appointed must have a Secret clearance.

2001. DUTIES AND RESPONSIBILITIES

1. MARRESFOR SECURITY Manager. The MARRESFOR Security Manager serves as the Commanding General's principal advisor and direct representative in matters pertaining to the security of classified information and personnel security. The MARRESFOR Security Manager ensures the implementation, supervision, and coordination of all activities related to information and personnel security. The MARRESFOR Security Manager will be appointed in writing by the Commanding General, and identified to all command personnel by listing the MARRESFOR Security Manager in organizational charts, telephone listings, rosters, etc. The MARRESFOR Security Manager will be guided in the performance of duties by the reference and this Manual.

2. Assistant MARRESFOR Security Manager. The Assistant MARRESFOR Security Manager will be designated in writing. This officer's duties are to assist the MARRESFOR Security Manager in all actions required to carry out the program as described in this Manual.
3. Headquarters Battalion, Security Manager (HqBn, SecMgr). The HqBn, SecMgr duties are limited to implementing, administering, and supervising the Personnel Security Program (including the processing of security investigation forms, maintenance of access rosters, data input and query in JUMPS/MMS/REMMPS, etc.) for members of this Headquarters and collocated MSC personnel assigned to the MARRESFOR Headquarters Battalion at New Orleans. This responsibility does NOT include the investigative requirements for Sensitive Compartmented Information (SCI) access which is retained by the MARRESFOR Special Security Officer (SSO). The HqBn, SecMgr will be guided in the performance of his duties by the appropriate references listed in appendix A and this Manual. The HqBn SecMgr will be appointed in writing by the Commanding Officer, Headquarters Battalion.
4. MSC Security Managers. The Headquarters of the 4th MarDiv, 4th MAW and the 4th FSSG are collocated with Headquarters MARRESFOR in New Orleans. These Security Managers are appointed in writing by their respective Commanding Generals. Their responsibilities include the development, implementation, and supervision of an Information Security Program (ISP) within their command EXCEPT those functions specifically assigned to the MARRESFOR or Headquarters Battalion Security Manager. MSC Security Managers are the Immediate Superiors in Command for their respective unit Security Managers. They will be guided in the performance of their duties by the reference, this Manual, and applicable directives listed in Appendix A.
5. Marine Corps Reserve Support Command (MCRSC) Security Manager. The MCRSC Security Manager will be appointed in writing by the Commanding General, MCRSC. Responsibilities include the development, implementation, and supervision of an ISP within that command. This includes the processing of security investigation forms, maintenance of access rosters, data input and query in JUMPS/MMS/REMPs, etc., for all personnel in the command. This responsibility does NOT include the investigative requirements for Sensitive Compartmented Information (SCI) access which is retained by the MARRESFOR Special Security Officer (SSO). He will be guided in the performance of his duties by the reference, this Manual, and applicable directives listed in Appendix A.
6. 2d and 3d Marine Expeditionary Brigades (2d & 3d MEB) Security Manager. The MEB Security Manager will be appointed in

writing by their respective Commanding Generals. Their responsibilities includes development, implementation, and supervision of the ISP within their command. This includes the processing of security investigation forms, maintenance of access rosters, data input and query in automated administrative systems for all personnel in that command, except those investigative requirements for SCI access. SCI access is the responsibility of the MARRESFOR SSO. These Security Managers will be guided in their duties by the reference, this Manual, and applicable directives listed in Appendix A.

7. Site Security Manager. Site Security Managers will be appointed in writing by the Unit Commander. They will be guided in the performance of their duties by the reference and this Manual.

8. Officer in Charge, MARRESFOR Classified Material Control Center (OIC, CMCC). The MARRESFOR CMCC is a consolidated CMCC that is responsible for all classified material for the Headquarters MARRESFOR, 4th MarDiv, 4th MAW, and 4th FSSG (except where noted otherwise). An officer and a senior Staff NCO (E7/8) of the MARRESFOR G-1 are assigned duties as the OIC and NCOIC of the CMCC. These assignments will be designated in writing by the MARRESFOR Adjutant. Except as specified otherwise within this Manual, the OIC, CMCC is responsible for the receipt, accounting, control, handling, transmission, and disposal of Secret and Confidential documents and materials held for which Headquarters MARRESFOR is accountable. Subordinate units, not located at MARRESFOR Headquarters, holding classified material will appoint an OIC or SNCOIC, CMCC for their location.

9. Secondary Control Point Custodian (SCPC)/Alternate Secondary Control Point Custodian (AltSCPC) and Secondary Control Point Clerk (SCPClk)

a. Each SCPC and AltSCPC will be appointed in writing by the Section Head of the section where the SCP is located. The SCPC will be a Staff NCO. The AltSCPC will be a NCO. All individuals assigned will have a security clearance and access commensurate with the highest level of classified material maintained by the SCP. No material higher than SECRET will be held in a SCP.

b. The SCPC is responsible for the operation of the SCP, for compliance with existing regulations, and section ADP security. The AltSCPC is responsible for assisting the SCPC in the performance of these duties. Subordinate units will appoint SCPC, AltSCPC, or SCPClk, as required.

10. Sub-custody Control Point Custodian (SCCPC) and Sub-custody Control Point Clerk (SCCPClk). Each SCCPC and SCCPClk (if appointed) will be appointed in writing by the Section Head

and will be a SSGT or above. Both will have a security clearance and access commensurate with the highest level of classification of classified material maintained in the SCCP. SCCPC's are responsible to their SCPC for the classified material under their charge and for compliance with existing security regulations. Currently no subordinate command holds the quantity of classified material that would require the establishment of a SCCP or Sub-custody Custodians.

11. Top Secret Control Officer (TSCO). A GySgt or above of the G-1 section will be assigned collateral duties as the TSCO. This assignment will be designated in writing by the MARRESFOR Adjutant. The TSCO is responsible to the MARRESFOR Security Manager for the receipt, custody, accounting for, and disposition of Top Secret material and Critical Nuclear Weapon Design Information (CNWDI) within MARRESFOR Headquarters. There are no subordinate commands that are currently authorized to hold Top Secret material and no TSCO appointment is necessary. The OIC, CMCC may also be appointed as the TSCO. The duties of the TSCO are listed in paragraph 2-10 of the reference, and as supplemented below:

a. Conduct a semi-annual (January and July) page-check, enclosure, and overlay inventory of Top Secret material for which they are responsible, with a report of such inventory delivered to the MARRESFOR Security Manager no later than the tenth of the following month. A joint inventory will be conducted upon appointment and relief of a TSCO. During the inventories, each document will be physically sighted.

b. Ensure that all personnel having access to Top Secret material are cleared from accountability prior to departure from the MARRESFOR Headquarters as a result of Permanent Change of Station Orders or Temporary Additional Duty exceeding 60 days. This requirement also applies to the outgoing TSCO. The relieved TSCO will not be released from the command until all Top Secret accounting discrepancies are resolved to the satisfaction of the new TSCO, MARRESFOR Adjutant, and the Commanding General. The new TSCO will then advise the MARRESFOR Adjutant of acceptance of the account in writing. The MARRESFOR Adjutant will endorse the letter, signifying appointment of the new TSCO and relief of the outgoing TSCO.

12. Top Secret Control Assistants (TSCA'S). The TSCO may appoint TSCA's to assist him. Appointments will be in writing and approved by the MARRESFOR Adjutant. TSCA's will be in the grade of Sgt or above and possess a Final Top Secret clearance. They may perform the following functions:

a. Sign courier receipts and transfer of custody receipts for Top Secret material.

b. Certify material being transferred into the Defense Courier System (DCS) and sign DCS Form 1 on behalf of the TSCO.

c. Transmit Top Secret material within MARRESFOR Headquarters.

d. Conduct required page checks of Top Secret documents.

13. NATO Sub-Registry Control Point Officer. A GySgt or above will be assigned duties as the NATO Sub-Registry Control Point Officer in writing by the OIC, CMCC. The Sub-Registry Control Officer will be guided in the performance of their duties by the reference.

14. COSMIC/ATOMAL Control Officer. The NATO Sub-Registry Control Point Officer is also assigned collateral duties as the COSMIC/ATOMAL Control Officer. The control officer will be guided in the performance of their duties by the reference.

15. Naval Warfare Publications Library (NWPL) Control Officer. A Sgt or above of the CMCC will be assigned collateral duties as the NWP Control Officer in writing by the OIC, CMCC and will be guided in the performance of their duties by the reference and this Manual.

16. ADP Security Officer. An officer of the Information Systems Management Office (ISMO) is assigned in writing collateral duties as the ADP Security Officer for MARRESFOR by the AC/S, G-6. The ADP Security Officer is responsible to the MARRESFOR Security Manager for the protection of classified information processed on automated systems, and assists the MARRESFOR Security Manager in the planning, establishment and supervision of a continuing ADP Security Program per the reference and this Manual. Subordinate units will assign an ADP Officer if their location processes classified information on any electronic or automated system other than a typewriter.

17. Communications Security Material System (CMS) Responsible Officer. As a senior staff officer within the command, the AC/S, G-6, is assigned collateral duties as the CMS Responsible Officer (RO) by the Commanding General, MARRESFOR. If further delegated, the CMS RO must be a field grade officer in accordance with Cryptographic Security Policy and Procedures (CSP-1A) and Communications Security Material System (CMS 4L). Regulations governing the protection of information and material are contained in the reference and this Manual.

18. CMS Custodian. A Staff Sergeant or above from the MARRESFOR G-6 section will be assigned the Primary Duty as CMS Custodian. The CMS Custodian and alternates will be assigned in writing in accordance with the provisions of the reference. Additionally,

the CMS Custodian and Primary alternate custodian will be trained and certified as CMS Inspectors responsible for inspecting CMS accounts of all subordinate units in accordance with the reference. The reference requires that collateral or additional duties assigned to the CMS Custodian must not interfere with the proper management of the CMS account.

19. Communications Security (COMSEC) Officer. The MARRESFOR Communications Electronics Officer (CEO) within G-6 is assigned collateral duties as the COMSEC Officer for MARRESFOR. This designation will be in writing by the AC/S, G-6. The COMSEC Officer is responsible for the planning, establishment, and supervision of a continuing COMSEC Program. The duties and functions of the COMSEC Officer are further described in the references listed in para. 18 above.

20. Special Security Officer (SSO). The MARRESFOR SSO will be an officer from the G-2 section. This assignment will be in writing by the Commanding General, MARRESFOR. The SSO coordinates his functions with the MARRESFOR Security Manager per DOD Directive C-5105.21 M1 (NOTAL). All MARRESFOR units will conduct direct liaison with the MARRESFOR SSO on all SSO and Sensitive Compartmented Information (SCI).

2002. TURNOVER FILES/DESKTOP PROCEDURES

1. Individuals assigned to duties described in paragraph 2001, above will prepare and maintain a Turnover File to facilitate the in-briefing of personnel assuming those duties. At minimum, such files will contain a copy of this Manual, copies of current appointment letters and endorsements thereto, copies of all official correspondence relevant to the position, copies of all custodial documents (inventories, receipts, destruction reports) or a memorandum indicating where they may be found, and a brief synopsis of the duties of the position.

2. Individuals appointed to positions of responsibility under this Manual will prepare and maintain a current desktop procedures folder. This folder will contain detailed instructions for the accomplishment of the duties inherent in their positions.

3. All supervisors will include in their turnover file information pertaining to their supervisory role in accomplishing the security policy and procedures set forth in this Manual.

2003. INSPECTIONS/INVENTORIES

1. In addition to other inspections directed or conducted by

higher headquarters, at least once annually, the MARRESFOR Security Manager will ensure that a detailed inspection of the CMCC, TS, NATO and NWPL accounts is conducted.

2. The OIC, CMCC will conduct a semi-annual inventory of SCP/SCCP's. This inventory will include all controlled material. The OIC, CMCC will report all inventory discrepancies/findings to the MARRESFOR Security Manager no later than the fifteenth of the month following the inventory.

3. The OIC, CMCC will conduct periodic inspections of each SCP. The OIC, CMCC will notify Section Heads and the appropriate Security Manager of corrective action required. A copy of the final results will be forwarded to the MARRESFOR Security Manager. For subordinate units the results will be forwarded to the Unit Commander. A comprehensive security inspection guide is contained in the reference. Security Inspection reports will be maintained by the SCP for two years and then destroyed.

4. The SCPC will conduct inspections of all SCCP's within the section, annually. Results will be reported to the Section Head, with information copies to the OIC, CMCC.

5. The ADP Security Officer, in coordination with the MARRESFOR Security Manager, will conduct periodic inspections and evaluations of ADP security procedures throughout the Headquarters and subordinate units in conjunction with annual inventory/inspections.

6. In addition to the Commanding General inspections, the MARRESFOR Security Manager will direct periodic Unannounced Security Inspections (USI) to be conducted throughout the Headquarters and subordinate units. These inspections will be conducted by personnel who have a Top Secret security clearance and possess a letter of authorization to conduct the USI signed by the Commanding General, MARRESFOR. The inspections will be conducted to determine if classified material is being afforded adequate physical protection and to evaluate compliance with security regulations. Violations and compromise will be reported and acted upon per chapter 4 of this Manual. Duty personnel will be provided with a copy of the letter designating personnel authorized to conduct USI's. The following procedures will govern the conduct of USI's:

a. Members of the inspecting team will present their U.S. Armed Forces Identification Cards, along with the Letter of Authorization to the Staff Duty Officer (SDO). If USMC Counterintelligence personnel are conducting the USI they will present official Marine Corps counterintelligence credentials which will be the only identification required of them.

SOP FOR ISP

OPNAVINST 5510.48J, "Manual for the Disclosure of Classified Military Information to Foreign Governments and International Organizations"

MCO 5510.14, "ADP Security Manual"

OPNAVINST C5510.93E, "Navy Implementation of National Policy on Control of Compromising Emanations"

MCO 5521.3H, "Personnel Security Investigations, Security Clearances, and Access"

ForO P5000.1 "Staff Regulations"

SOP FOR ISP

APPENDIX A

LIST OF REFERENCES

OPNAVINST 5510.1H, "Department of the Navy Information and Personnel Security Program"

CMS 4-L, "Communications Security Material System"

CSP-1, "Cryptographic Security Policy and Procedures"

OPNAVINST C5605.19, "Automated Distribution List of COMTEC and JCS Pubs for Operational Forces of the Navy"

NWP O, "Naval Warfare Documentation Guide"

OPNAVINST 5513.1C, "Department of the Navy Security Classification Guidance"

OPNAVINST C5510.101D, "NATO Security Procedures"

NTP-4, "Fleet Communications"

OPNAV NOTICE 5510 09N2/1U529998 dtd 31 Dec 91, "Destruction of Secret Messages"

OPNAVINST 5239.1A, "Department of the Navy Automatic Data Processing Security Program"

SECNAVINST 5720.44A, "Department of the Navy Public Affairs Regulations"

MCO 5510.9A, "Security Review of Information for Public Release"

DOD 5210.2, "Access to/and Dissemination of Restricted Data"

OPNAVINST S5511.35J, "Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U)" (NOTAL)

OPNAVINST 5530.14B, "Physical Security and Loss Prevention" (NOTAL)

OPNAVINST 4650.11E, "Official Temporary Duty Travel to Military and Civilian Installations, Activities, and Units; Policy and Procedures for"

Classified information will not be transmitted over the LAN nor will classified material be processed on a system connected to the LAN. The LAN must be physically disconnected from the system before classified material may be processed.

12009. COMPUTER VIRUSES

1. A computer virus is a computer program which, once in a computer, performs certain functions when a "trigger event" occurs, such as a certain date or time in the computer's clock. The virus' actions may be harmless, such as displaying a message on the screen, or destructive, such as wiping out a hard disk.
2. A virus enters a computer through modems, bulletin boards or infected floppy disks.
3. To minimize the impact of a virus, maintain frequent backups of your data. If a virus destroys your hard disk, you can restore your data from the backup and your programs from the original program diskettes.
4. Personnel suspecting a computer virus on a system that processes classified material should immediately report the problem to the MARRESFOR ADPSO.

media is returned to the CMCC for destruction, a receipt for the media will be obtained and filed with the ADP binder.

3. The following is an example of an ADP inventory sheet:

DISK # NAME	FILE CREATED	CLASS	DATE	OFFICE	SUBJECT
02156	001-89	S/NF	2 JAN 89	OPS	OPLAN 1000 (DRAFT)
02189	002-89	C	2 JAN 89	SPECOPS	OPSEC THREAT

12006. DECLASSIFYING, CLEARING, OR DESTROYING ADP DATA

1. Controlled diskettes and removable hard disks will not be downgraded, upgraded, or declassified. All controlled diskettes and removable hard disks will be turned in to the CMCC for destruction. Destruction will be recorded on an appropriate destruction report.

2. Unclassified system diskettes and diskettes containing executable programs will be write-protected before they are inserted into a system which is processing classified data. Non-controlled diskettes used for processing only unclassified information will be destroyed by incineration or shredding.

3. Random Access Memory (RAM) is the transient memory resident in the central processing unit of a computer. This memory is only active when power is supplied to the system. After classified data has been processed, and before data of any other classification level may be processed, RAM must be cleared of all data. This is accomplished by POWERING OFF all components of the system three times for a minimum period of ten seconds each.

12007. TRANSMISSION EQUIPMENT/CLASSIFIED DATA. No transmission equipment (i.e., STU III, modems, LAN cables, etc.) will be connected to ADP equipment used to process classified data unless approved in writing by the Security Manager. A request to connect such equipment will be submitted to the Security Manager via the ADPSO. This request will contain the nomenclature of the equipment to be connected and the justification. Upon receipt of the request, the ADPSO will evaluate the request based on the equipment to be used and justification and endorse the request with comments and a recommendation to the Security Manager.

12008. LOCAL AREA NETWORK (LAN). The LAN is used to transmit unclassified information to sections within this Headquarters.

5. When a diskette is to be used, the entire folder containing the diskette and inventory sheet will be maintained together. As a file is added to the diskette, the inventory sheet for that particular diskette will be annotated accordingly and a copy of the sheet will be provided to the SCP custodian for inclusion in the ADP Binder. The inventory sheet should be stapled to the folder to prevent loss. (See paragraph 13005, below.)

6. Prior to writing classified data to a removable hard disk or other magnetic media, the media will be taken to the CMCC to be assigned a control number and marked with a Data Descriptor Label and the appropriate Magnetic Media Classification Label for the highest classification of data authorized for storage on the media.

7. All controlled magnetic media will be stored in GSA approved containers when not in use, and afforded the full protection required for a classified document of the same classification.

8. All controlled magnetic media will be included in semiannual, change of custodian, and other required inventories. Controlled magnetic media will be returned to the CMCC for destruction.

9. NO CLASSIFIED DATA WILL BE CREATED, PROCESSED ON, OR COPIED TO (EVEN TEMPORARILY), A NON-REMOVABLE DRIVE UNLESS SPECIFIC APPROVAL HAS BEEN OBTAINED IN ACCORDANCE WITH MCO 5510.14 (ADP SECURITY MANUAL) AND THIS MANUAL.

10. All printer and typewriter ribbons will have labels placed on them noting the appropriate classification level. Typewriter and printer ribbons used in the printing of classified information will be locked in a GSA approved security container at the end of each work day. Printer ribbons and typewriter ribbons will be returned to the CMCC for destruction.

12005. ADP BINDER

1. An ADP Binder is required to maintain a record of classified files maintained on magnetic media. The purpose of the binder is to enable the command to determine what classified information may be subjected to compromise in the event a disk becomes lost/missing.

2. The binder will be located at the SCP/SCCP and contain a copy of the diskette inventory sheet on all diskettes held by the SCP/SCCP. The diskette inventory sheet will at a minimum contain the following information: file name, classification, subject, date created, disk bucktag number, and creator of the file (this may be the office code). Unclassified subject titles will be used to preclude classification of the ADP binder. When magnetic

REPORT UNAUTHORIZED USE OR ACCESS TO THE SYSTEMS OR ADP SECURITY OFFICER.

WARNING ** CAUTION ** WARNING ** CAUTION ** WARNING

This warning, when flashed on the screen, must force the user to hit some key or take some action to clear the screen of the message. Software and assistance to implement this procedure may be obtained from the ADP Security Officer (ADPSO).

5. Monitors will be checked frequently for "burn in". Burn in results when monitors are left on for extended periods of time and data remains on the screen after the monitor is turned off. All systems will have a burn in program installed in their system to help prevent burn in. Software and assistance may be obtained from the ADPSO.

12004. DATA SECURITY

1. All floppy diskettes will be color coded according to the highest classification of the data on them. The following color codes will be used: BLUE = CONFIDENTIAL; RED = SECRET; ORANGE = TOP SECRET; YELLOW = SCI. The OIC, Classified Material Control Center is solely responsible for ordering, stocking and distributing BLUE (confidential), RED (secret), and ORANGE (top secret) diskettes. Only the Special Security Officer (SSO) is authorized to order and stock SCI (yellow) diskettes. Yellow diskettes will not be removed from the SSO spaces. Blue, Red, Orange, and Yellow diskettes will not be used for processing "UNCLASSIFIED" material.

2. All diskettes (except black) will be formatted and assigned a bucktag number at the CMCC prior to distribution to a section. During formatting the bucktag number will be assigned as the volume label. The control number assigned by the CMCC will be written on the diskette jacket using an indelible ink marker. Ball-point pens will not be used because of the potential damage to the floppy disk magnetic medium. SCI (Yellow) diskettes will be marked in the same manner by the SSO.

3. Once assigned a bucktag number, the diskette will be placed in an appropriate colored folder with a diskette inventory sheet and CMCC Control Card.

4. The folder containing the diskette and inventory sheet will be signed over to SCP's utilizing CMCC Control Cards. The same procedure will be utilized when transferring diskettes from the SCP to SCCP.

2. Locally developed applications (Class II) programs produced by the MARRESFOR ISMO will be stored on black diskettes. These programs will be clearly marked as Unclassified.
3. All vendor supplied software diskettes will be write protected before storing. This involves placing a write-protect-tab over the write protect notch on the top of the diskette. This will prevent any unintentional erasing of data.

12003. SYSTEM SECURITY

1. Systems will be operated in "Systems High Mode." That is when the system is processing classified information, only those individuals possessing the requisite clearance for the highest classification of data in the system (or any media accessible through the system), and possessing the need-to-know for any of the information accessible through the system, will be allowed access to the system.
2. Privately owned systems are not authorized to process classified information. In addition, privately owned software or public domain software from non-government sources is not authorized to process classified information. This security measure is intended to prevent a computer virus or other form of system contamination from occurring. Classified information will only be processed on U.S. Government equipment, in secure work spaces.
3. Environmental controls will be in accordance with the manufacturer's specifications. Sustained operation at the extremes of the manufacturer's suggested ranges may result in degraded equipment performance.
4. All microcomputer systems users will ensure that a warning logo is flashed on the screen upon initial entry to the system. This logo will contain the following message:

WARNING ** CAUTION ** WARNING ** CAUTION ** WARNING

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT
COMPUTER AND/OR SOFTWARE IS PROHIBITED BY PUBLIC LAW 98-473

Public Law 98-473, Chapter XXI, Paragraph 1030 states that,
"Whoever knowingly accesses a computer without authorization, or
having knowingly accessed a computer authorization,
...obtains, uses, modifies, destroys, or discloses,
or prevents authorized use of (data or a computer owned by or
operated for) the Government of the United States ... shall be
punished (by) ...a fine ... or ... imprisonment. ."

SOP FOR ISP

CHAPTER 12

AUTOMATED DATA PROCESSING SECURITY PROCEDURES

12000. BASIC POLICY. Automated Data Processing (ADP) security is the responsibility of every ADP user in this headquarters. This responsibility includes the use and handling of all word processing equipment, ADPE-FMF equipment, desktop microcomputer systems, on-line terminals, and the Fleet Marine Force-End User Computing Equipment (FMF-EUCE) machines.

12001. PROCESSING CLASSIFIED DATA

1. The procedures for handling and processing classified information on office automation equipment are generally the same as the procedures for typing classified material on a manual typewriter. All diskettes, printer ribbons, printouts, and any other products of classified information processing will be treated as classified material and handled per the reference and MCO 5510.14 (ADP Security Manual).

2. Before any automated system can be used to process classified data, the system must be accredited. Requests for authorization to process classified data shall be submitted to the ADP Security Officer. For non tempest systems processing classified information at the SECRET or higher level, accreditation may only be granted after submission of a TEMPEST Vulnerability Assessment Request (TVAR) per the reference. Other actions required during the accreditation process are detailed in the OPNAVINST C5510.15E and OPNAVNOTE C5510 dated 13 October 1990.

3. Office automation users shall possess the proper security clearance and access for the highest classification of data processed in the system and possess the need to know for any of the information accessible through the system. Each component for the system shall be powered off and on three times for a minimum of 10 seconds each before processing a different level of classification.

12002. SOFTWARE SECURITY

1. Vendor application packages such as Enable, Wordstar, DBase III, and SuperCalc are delivered to the user on black diskettes and are clearly marked. These packages will be stored in a manner to preclude theft. No additional markings will be required on vendor supplied diskettes. These diskettes will be treated as unclassified. These diskettes should be copied to backup diskettes and protected accordingly as backup copies.

SOP FOR ISP

CHAPTER 12

AUTOMATED DATA PROCESSING SECURITY PROCEDURES

	PARAGRAPH	PAGE
BASIC POLICY	12000	12-3
PROCESSING CLASSIFIED DATA	12001	12-3
SOFTWARE SECURITY	12002	12-3
SYSTEM SECURITY	12003	12-4
DATA SECURITY	12004	12-5
ADP BINDER	12005	12-6
DECLASSIFYING, CLEARING, OR DESTROYING ADP DATA	12006	12-7
TRANSMISSION EQUIPMENT/CLASSIFIED DATA . .	12007	12-7
LOCAL AREA NETWORK (LAN)	12008	12-7
COMPUTER VIRUSES	12009	12-8

SOP FOR ISP

SINGLE SCOPE BACKGROUND INVESTIGATIONS
PAPER TRAIL

SSBI / GENSER

= Eligible for TS

SSBI / SCI

= Eligible for TS/SCI

DONCAF

SSO Navy/SECGRU

DIS

DIS

Site SecMgr

MRF SSO

Most clearances in MRF
e.g. BN/SQDN I-I's. CO's
XO's, S-3s

Site SecMgr

02XXs & 26XXs

INVEST/CLEARANCE=SSBI/TS

INVEST/CLEARANCE=SSBI/TS/SCI

Figure 11-5.--Single Scope Background Investigations
Submission Procedures.

SOP FOR ISP

HEADING

5520
Sect:
Date

MEMORANDUM

From: Headquarters Battalion Security Manager
To: Section Head

Subj: REQUEST FOR CLEARANCE/ACCESS TO CLASSIFIED MATERIAL;
(RANK/NAME/SSN/MOS/STATUS/PLACE OF BIRTH)

Ref: (a) OPNAVINST 5510.1H
(b) Section Memo

1. Per the references, the above named individual was granted an (INTERIM/FINAL) clearance/access on (date) based on a submitted request for clearance to Department of the Navy, Central Adjudication Facility through the unit diary.
2. Interim clearance will expire on (date) or upon response from the above request.
3. Subject (is/is not) authorized to receipt for classified material.

SIGNATURE

Copy to:
OIC, CMCC

Figure 11-4.--Request for Clearance/Access to Classified Material.

SOP FOR ISP

HEADING

5520
Sect:
Date

MEMORANDUM

From: Headquarters Battalion Security Manager
To: Unit Diary Clerk

Subj: REQUEST FOR JUMPS/REMMPS/MMS ENTRY

Ref: (a) CMC ltr 1080 MPI-52 dtd 24 Mar 88
(b) CMC ALMAR 099/88
(c) MCO P1080.35, para 8090 (PRIM)
(d) Section Memo

1. Per the references, it is requested that the following administrative action be taken concerning:

<u>RANK</u>	<u>NAME</u>	<u>SSN</u>	<u>PLACE OF BIRTH</u>
<u>ACTION</u>	<u>CODE</u>	<u>REASON</u>	
_____	A	REQUEST CONFIDENTIAL CLEARANCE	
_____	B	REQUEST SECRET CLEARANCE	
_____	C	REQUEST TOP SECRET CLEARANCE	
_____	F	REQUEST TERMINATION OF CLEARANCE	
_____	G	REQUEST TERMINATION OF CLR FOR CAUSE	
_____	H	REQUEST REVOCATION OF CLEARANCE	
_____	I	REQUEST CLEARANCE STATUS	

FIRST ENDORSEMENT

From: Unit Diary Clerk
To: Headquarters Battalion Security Manager

1. Clearance/Access entered on UD# _____ dated _____.

Copy to:
File

SOP FOR ISP

HEADING

5520
Sect:
Date

MEMORANDUM

From:
To: MARRESFOR HQBN Security Manager
Subj: REQUEST FOR PERSONNEL SECURITY CLEARANCE

(RANK/NAME/SSN/MOS/STATUS/PLACE OF BIRTH)

Ref: (a) OPNAVINST 5510.1H

1. Per the reference, it is requested that a personnel security clearance to the level of (circle one) CONFIDENTIAL/SECRET/TOP SECRET be granted in the case of the above named individual. This individual will require access to classified information while in the performance of assigned duties.

(SECTION HEAD)

Copy to:
FILE

Figure 11-2.--Request for Access to Classified Information.

SOP FOR ISP

PERSONNEL SECURITY ACTION REQUEST			
Part I - Subject Information <i>Items 1 thru 11 MUST be completed</i>			
1. Name (Last, First, Middle)	2. Social Security No.	3. Grade/Rank	4. Status
5. Former Name(s) / Alias(es)	6. Date of Birth (YYMM/DD)	7. Place of Birth (State/Country)	
8. Residence (Complete Mailing Address)		9. Citizenship a. United States <input type="checkbox"/> By birth <input type="checkbox"/> Naturalized <input type="checkbox"/> Born of U.S. citizens outside of the U.S. b. Other: _____	
10. UIC (Submitting Unit)		11. UIC (Responsible)	
Part II - Request for Security Clearance / Eligibility Determination <i>If you are requesting a clearance, items 12 thru 15 and 17 thru 19 MUST be completed. Please attach OPNAV 5570/120 if available.</i>			
12. Local Records Certification <input type="checkbox"/> Favorable <input type="checkbox"/> Unfavorable (See remarks below) <i>I certify completion of checks of local personnel, legal, medical, base/military police, security and other command records about the subject as noted above.</i>		13. Continuous Federal Service Certification <i>I certify that subject has been in continuous federal service without a break exceeding 12 months since _____</i>	
14. Interim: _____ clearance granted based on _____ to expire on _____			
15. Action Requested Regarding Subject: <input type="checkbox"/> CONFIDENTIAL <input type="checkbox"/> SECRET <input type="checkbox"/> TOP SECRET <input type="checkbox"/> Non-Critical Sensitive (Civilian) <input type="checkbox"/> Critical Sensitive (Civilian) <input type="checkbox"/> Other: _____			
16. REMARKS - ENCLOSURES (Attach pages as necessary)			
17. Date	18. Name, Grade/Rank, Title and Autocon No. Commercial No.	19. Signature	
Part III - Change in Status Report <i>Complete EITHER 20a, 20b, OR 20c. You must complete 21 thru 23.</i> <i>If item b is marked or if item c involves significant unfavorable information, you MUST attach ALL available documentation.</i>			
20. Action Taken a. Subject's clearance was lowered without prejudice to <input type="checkbox"/> NO CLEARANCE <input type="checkbox"/> CONFIDENTIAL <input type="checkbox"/> SECRET b. Subject's access to classified information suspended for cause (Report attached) c. Other: _____			
21. Date	22. Name, Grade/Rank, Title and Autocon No. Commercial No.	23. Signature	

OPNAV 5510-411-1-101

64-0101-1-101-420

Figure 11-1.--Personnel Security Action Request.

signed, and indoctrination completed. Any questions pertaining to SSBI submissions for SCI access should be addressed to the MARRESFOR SSO/TCO at DSN: 363-6510/Comm: (504) 942-6510.

5. See chapter 9 and paragraph 11003.7 of this Manual, and chapter 21 of the reference for information regarding the completion and submission of the SSBI package. Any questions pertaining to SSBI submissions for TS clearances and below should be addressed to the MARRESFOR Security Manager DSN: 363-6961/Comm: (504) 942-6961 or at DSN: 363-6108/Comm: (504) 942-6108.

6. Once SSBI documentation has been submitted to the SSO the local Security Manager may authorize an interim Top Secret clearance if access to GENSER level Top Secret material is required. Procedures will be the same as outlined in paragraph 11015.3f.

11023. MOBILIZATION AND SCI ACCESS

1. All Battalion/Squadron Commanders, Executive Officers, Operations Officers, and other key billet holders should have an up to date adjudicated SSBI submitted through DIS to DONCAF prior to mobilization per paragraph 11003.5 above.

2. Upon notice of mobilization the unit Security Manager will notify MARRESFOR SSO of the identity of the gaining command. MARRESFOR SSO will coordinate with the gaining command SSO to determine SCI requirements. If a requirement for SCI access exists, SSO Navy will be notified.

3. SSO Navy will coordinate with DIS (info DONCAF) to acquire SSBI results held for GENSER clearance. SSO Navy will then evaluate the SSBI to SCI standards for adjudication. Upon adjudication MARRESFOR SSO and the gaining command SSO will be notified as to the Marine's SCI eligibility.

4. For Marines believed to require SCI access at mobilization who have not submitted an SSBI, the local Security Manager will notify the MARRESFOR SSO for further instructions. A MARRESFOR SSO Contact Team will also augment the Reserve Support Unit (RSU) at the Site of Initial Assignment (SIA) to coordinate SSO administrative duties and requirements.

conditions". A determination must be made as to whether or not these Marines' security clearances will be terminated. If the security clearance is terminated, then the action must be completed prior to the Marines' release from active duty.

11020. TERMINATION OF ACCESS. Access to classified information and/or equipment will be terminated immediately when the individual no longer requires knowledge or possession of classified information or equipment in order to accomplish their assigned mission, the individual leaves the section, or the individual becomes ineligible to maintain a security clearance.

11021. VISITOR AUTHORIZATION REQUESTS. When the Security Manager learns that the unit/section is to be visited by cleared personnel he should be notified, by letter, from the visitors' security office, of all pertinent clearance and investigation data on the subject individual(s). Security Manager will verify all such clearance data with DONCAF, make endorsement to the original letter (Subj: VERIFICATION OF CLEARANCE FOR VISITOR AUTHORIZATION REQUEST) for the section head of the section being visited, and keep one copy for the Security Manager's files. The Security Manager's endorsement will include the time period of the visit.

11022. INVESTIGATION REQUIREMENTS FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION (SCI)

1. The Single Scope Background Investigation (SSBI) is the standard investigative prerequisite for access to Top Secret (TS) information, access to Sensitive Compartmented Information (SCI) and civilian assignment to critical-sensitive/special sensitive positions.
2. The security, use, and dissemination of Special Intelligence (SI) is accomplished through the MARRESFOR SSO and the Tango Control Officer (TCO).
3. The MARRESFOR SSO/TCO is responsible for:
 - a. The management of the SCI billet structure. (This billet structure is a listing of positions for which the need-to-know for access has been approved.)
 - b. The granting of clearance and access to SCI material.
4. Access to SCI will be denied until need-to-know is approved, eligibility determined, SCI Non-Disclosure Agreement (NDA) is

a. Advise the individual, in person, when limiting or suspending his/her access. The reason for limitation or suspension may or may not be given to the individual, as deemed appropriate by the Commanding Officer;

b. Take steps to ensure that the individual's name is removed from the access roster, or limitations noted on the access roster, and that all coworkers are notified of the limitation or suspension;

c. Notify the Security Manager to ensure that the combination to classified storage containers, to which the individual had access, are changed and that all classified material has been recovered from the individual;

d. Forward any derogatory information is to DONCAF for appropriate adjudication;

e. For Marines with MOS of 02XX or 26XX, notify MARRESFOR SSO and forward same information provided to DONCAF;

f. Restrict the reason/circumstances underlining any limitation or suspension of access so as to not become common knowledge among the subject's peers and/or subordinates.

11019. DENIAL/WITHDRAWAL OF SECURITY CLEARANCE FOR CAUSE

1. Paragraph 22-2 of the reference outlines the security criteria which would make an individual ineligible for a security clearance and serves as the basis for the withdrawal of a security clearance by the Security Manager. Paragraphs 23-8 and 23-9 of the reference, as well as paragraph 15 of the reference, outlines the procedures to be followed for denial/withdrawal of an individual's security clearance.

a. MARRESFOR General and Special Staff Officers, Commanding Officer, HQBN, and Officers In Charge/Supervisory Personnel will inform the MARRESFOR SecMgr or Unit Security Manager, as appropriate, on any act or incident which makes an individual ineligible to maintain a security clearance. A recommendation must be included as to whether or not the individual should retain their security clearance.

b. The Commanding Officer, HQBN, MARRESFOR and administrative supervisors within subordinate units will ensure that the MARRESFOR Security Manager or Unit Security Manager, as appropriate, is aware of all Marines with security clearances pending disciplinary action, administrative discharge boards, or being released from active duty under "other than honorable

paragraph 24-6 of the reference.

11017. ACCESS BY RESERVE PERSONNEL

1. Reserve personnel in an "active status" may be granted access to classified information as necessary for active duty for training or inactive duty training, if they hold the appropriate clearance. A record of access granted should be maintained by the Security Manager and the CMCC.

2. Reserve personnel may be given access to training editions of codes, cipher systems, authentication systems, call sign encryption systems, operating instructions, and maintenance manuals, as required to maintain proficiency in their specialties. Access to other COMSEC publications may also be granted.

3. "Inactive status" reserve personnel are not eligible for access to classified information unless specifically authorized by CNO (OP-09N) under the procedures identified in chapter 24 of the reference. Inactive status occurs when the individual is placed on the Reserve Inactive Status list by the Commandant of the Marine Corps.

4. Temporary access: This can be authorized by the Unit Commander for a Marine (regular or reserve) whose records indicate that the appropriate investigation has been conducted but no clearance has been issued. The purpose of this provision is to alleviate the administrative burden of processing an individual for a security clearance/access when it is only needed for a limited time period, usually 10 days or less. However, since the clearance granting process for Marines is now automated little time, if any is saved by using this procedure. It may be more appropriately used for Navy personnel assigned to Marine Commands since their clearance procedures are not yet fully automated. Paragraph 24-5 of the reference has additional information on this subject.

11018. SUSPENSION OF ACCESS

1. When questionable or unfavorable information becomes available concerning an individual who has been granted access, the Security Manager and Staff Judge Advocate (SJA) may decide to limit or suspend access. Limitation or suspension of access for cause may only be used as a temporary measure until the individual's eligibility for access has been resolved.

2. When effecting limitation or suspension of access, the Commanding Officer will:

d. The Security Manager submits (Figure 11-3), Unit Diary Request, to the unit diary clerk;

e. Using the MMS (JUMPS/REMMPS), the UD clerk enters the appropriate code for clearance action.

f. After the MMS entry has been completed, and the unit diary clerk has endorsed the UD request, the unit Security Manager may grant interim clearance/access for up to 180 days, pending DONCAF determination to grant a final clearance. (Navy personnel shall have a DD Form 5510/413, (Figure 11-1) forwarded to DONCAF by the Security Manager. Granting of interim clearances, (the filling out of Figure 11-5) shall be the same as for Marines. No other action is required, unless an extension is necessary, until notification by DONCAF. The access request is then endorsed accordingly by the unit Security Manager, and forwarded to the OIC/NCOIC, CMCC, with a copy to the original requester.

g. The OIC/NCOIC, CMCC, will have the individual execute an Indoctrination Brief and the Standard Form 312 (Rev. 1-91) Nondisclosure Agreement, as required. All briefing/orientation should be done at this time. At check-out, OIC/NCOIC, CMCC, will debrief the leaving individual (transfers). Individuals who are retiring, or leaving active service, will be debriefed by the unit Security Manager, who will then execute OPNAV 5511/14 (Rev. 7-78) Security Termination Statement. The Security Manager, will use (Figure 11-3) to request unit diary action to terminate clearances.

4. Access Listing

a. Each section will maintain, and keep current, a listing of personnel in their section authorized access to classified information or equipment.

b. The OIC/NCOIC, CMCC, will maintain a listing of all unit personnel authorized access to classified material or equipment as well as individuals who have receipt authority to draw classified material directly from the CMCC.

11016. ONE-TIME ACCESS. An urgent operational or contractual emergency may arise for cleared personnel to have one-time or short duration access to classified information at a higher level than that for which they are eligible. Therefore, for compelling reasons, in furtherance of the DON mission, an individual may be granted access at one level of classification above that for which eligible, subject to the terms and conditions outlined in

individual of the command has been granted access, the OIC/NCOIC, CMCC will ensure that the subject individual is given a security orientation briefing before being granted access to classified material. Chapter 3 of the reference details areas to be covered in this briefing. The OIC/NCOIC, CMCC will also ensure that the subject individual has executed Standard Form 312 (1-91), and that the document has been properly witnessed. A pg 11 entry in subjects OQR/SRB will be made as to the execution of the SF 312. The original SF 312 will be retained locally until the individuals transfer or separates. It will then be mailed to HQMC (code MMRB-20).

11015. REQUESTING AND GRANTING CLEARANCES

1. Commanding Generals, Commanding Officers, Unit Commanders and Security Managers are the only individuals authorized to grant access to classified information and equipment within the MARRESFOR and its subordinate units.

a. General and Special Staff Officers, Commanding Officer, Headquarters Battalion, Officers In Charge/Section Heads. These individuals will review their access requirements and report them to the OIC, CMCC and appropriate Security Manager. MARRESFOR SSO will handle all SCI access requests.

b. Subordinate Unit Commanders. These individuals will review their access requirements for daily operations within the unit's staff and those requirements for AT's or schools.

2. Access Requests. All access requests will be forwarded to the appropriate Security Manager.

a. If approved, the original request, bearing the Security Manager's endorsement, will be forwarded to the CMCC for retention. A copy will be retained for the Security Manager's files and a copy returned to the requesting OIC/Section Head for their files.

3. The steps to be taken in granting access are:

a. OIC/Section Head determines the level of access necessary for the individual to perform his/her duties;

b. Submit the Request For Access to appropriate Security Manager;

c. The Security Manager reviews local records for disqualifying information;

3. Interim clearances are effective for up to 180 days. Interim clearances may be extended by the unit Security Manager for an additional 180 days. Tracer actions for Marine Corps personnel will be made through the Manpower Management System (MMS) to DONCAF. (See paragraphs 21-15(5), 21-15(5)(c), 23-3, and 21-15(5)(e) of the reference for additional information.)

4. Should tracer action reveal that an investigation is not pending, nor any evidence exists to indicate that the requested investigation had been initiated by the investigating agency, the entire investigation request/questionnaire package shall then be resubmitted by the unit Security Manager. The interim clearance may be continued per the requirements set forth in paragraph 11012.2 of this Manual.

5. A final eligibility determination/adjudication will be made by DONCAF upon satisfactory completion of the requested personnel security investigation and will be reported via the Manpower Management System (MMS).

11012. NATO SECURITY CLEARANCE. Clearance/access to NATO classified information shall be based on a U.S. security clearance, granted for classified information of equivalent level, under the investigative requirements of paragraph 21-5 of the reference.

11013. NAVAL WARFARE PUBLICATIONS (NWP) SECURITY CLEARANCE. See paragraph 10-5 of the reference.

11014. ACCESS

1. Knowledge or possession of classified material or equipment shall be limited and permitted only to those individuals whose official duties require access to classified information or equipment in order to accomplish their assigned missions, and only to those individuals who have been issued a security clearance and determined to be eligible for access.

2. No one has a right to have access to classified information solely because of rank, position, or security clearance. The responsibility for determining whether a person's official duties require access to classified information rests upon the individual who has the authorized possession, knowledge, or control of the information involved and not upon the prospective recipient.

3. Upon notification by the unit Security Manager that an

manner, for final adjudication. This process should be coordinated by the unit Security Manager, or MARRESFOR SSO, as appropriate.

11010. GRANTING CLEARANCES

1. DONCAF is the sole authority for granting final security clearances (Genser level) for Navy and Marine Corps personnel.
2. Interface with DONCAF for security clearance actions shall be accomplished via the JUMPS/REMMPS on all Marine Corps personnel. Navy personnel will require the submission of OPNAV 5510/413, Personnel Security Action Request (Figure 11-1) to DONCAF for clearance action.

11011. INTERIM AND FINAL CLEARANCES

1. Security clearances are of two types:
 - a. Final Clearance. One granted by DONCAF upon the completion of all investigative requirements and adjudication.
 - b. Interim Clearance. One granted by the HQBN or local Security Manager temporarily, based on lesser investigation, pending completion of the full investigation requirements, or awaiting final clearance/adjudication action by DONCAF.
2. Interim clearances may be granted only after:
 - a. OIC/Section Head submits (Figure 11-2) to MARRESFOR HQBN Security Manager or unit Security Manager, requesting clearance and access at a specified level;
 - b. A unit diary entry requesting a clearance from DONCAF has been submitted, (Figure 11-3) from the unit Security Manager to the Unit Diary Clerk;
 - c. The required investigation request/questionnaire forms for final clearance have been sent to DIS/PIC, and a check of local records (personnel and medical) does not reveal information which clearly indicates that the individual is not a suitable candidate for a position of trust. The review of local civilian law enforcement records, the National Crime Information Center (NCIC), and the NCIS is prohibited.
 - d. Ascertaining that a favorably completed ENTNAC or NAC is already on file at DONCAF.

(

)

Questionnaire; FD 258, Fingerprint Card (two of them) (A DD Form 398-2 (with "31 Dec 93" typed in the upper right-hand corner of the form itself), Personnel Security Questionnaire (with items 1 through 8 completed) on spouse and immediate family members who are foreign nationals, immigrant aliens, resident aliens, or Nationalized U.S. citizens.

b. ENTNAC/NAC - DD Form 398-2 (with "31 Dec 93" typed in the upper right-hand corner of the form itself), and FD 258 (only 1).

3. When it has been determined that an individual requires an investigation for further issuance of clearance/access, the following procedures will be followed:

a. The individual will be notified by his/her Security Manager that a PSI (or PR) is required. The subject individual will be provided with the necessary forms as required by the proper investigation, and a copy of a detailed instructional guide (exhibits 21B through 21J of the reference).

b. The individual will complete the forms, legibly, in black ink, or typewritten.

c. Unit Security Managers will ensure that all forms are completed properly and that the entire investigation package is forwarded (with copies, as required) to the appropriate agency.

d. Unit Security Managers will provide one copy of the completed investigation request/questionnaire package to the individual and keep one copy of same for their files in case tracer action may be required before final adjudication by DONCAF, and/or loss of the investigation package occurs.

11008. REPORTS OF INVESTIGATION. Reports of investigation for ENTNAC's, NAC's, and SSBI's (for other than SCI access) are forwarded from the investigating agency to DONCAF for adjudication of a final clearance. Reports of investigation for SSBI's for access to SCI are forwarded through MARRESFOR SSO to COMNAVINTCOM or COMNAVSECGRU for adjudication. If the results of investigation are inadvertently returned to the original requester by DIS/PIC (in the case of GENSER level requests), they must be immediately forwarded to DONCAF.

11009. REQUESTS FOR ADDITIONAL INFORMATION Periodically, a completed investigation being adjudicated at DONCAF may contain information that requires expansion. In these cases DONCAF will forward additional investigative forms to the requesting command for the individual to complete and return to DONCAF, in a timely

2. Requests for PSI's shall be initiated only when:
 - a. There is no PSI on file with DONCAF on the individual;
 - b. It is necessary to provide the investigative basis required for the level of clearance/access, position, or duties.
3. Before initiating an investigation, unit Security Managers shall determine:
 - a. That the individual does not already have a valid investigation which would satisfy the requirement(s);
 - b. That the individual is in fact a U.S. citizen and;
 - c. That the OQR/SRB and medical records do not contain information which clearly indicates that the subject individual is not a proper candidate for a position of trust (Local records checks of police or NCIS files are not authorized.).
4. PSI's shall not be requested for individuals with less than nine months of active service remaining.
5. The preparation and submission of requests for investigation (except for SSBI/SSBI-PR's for SCI access) shall conform with paragraph 21-14 and exhibits 21B through 21J (as appropriate) of the reference. SSBI/SSBI-PR's for SCI access shall be submitted through the MARRESFOR SSO.
6. Figure 11-5 describes the submission chain for SSBIs for GENSER and SCI. Questions should be addressed through the appropriate chain as per paragraphs 11022.4 and 11022.5 of this chapter.

11007. PREPARATION AND SUBMISSION OF INVESTIGATION REQUESTS

1. Investigation requests are to be submitted on the forms indicated below and prepared according to the detailed instructions in exhibits 21B through 21J of the reference. The investigations required for clearance are as follows:
 - a. Top Secret - SSBI (GENSER level).
 - b. Secret/Confidential - ENTNAC or NAC (GENSER level).
2. The following are the forms required for each investigation:
 - a. SSBI - DD Form 1879 (Mar 90), Request for Personnel Security Investigation; DD Form 398 (Mar 90), Personnel Security

7. Investigation requirements for all Marine Corps personnel in MOS 02XX and 26XX shall have an SSBI completed or updated within the last five years submitted via MARRESFOR SSO. (See Paragraph 11022)

8. Validity of Prior Investigations. A Personnel security investigation (SSBI, PR, NAC or ENTNAC) completed by an agency of the federal government remains valid unless the individual has had a break in continuous service for a period greater than one year. Continuous service consists of honorable active duty including military reserve forces (ready reserve or stand-by reserve not officially placed on the Inactive List), National Guard, Air National Guard, ROTC, etc.

9. Verification of Investigation

a. To determine if an individual has a completed personnel security investigation, view the individuals MS21 page of the Visual Inquiry System (VIS) or the Basic Training Record (BTR). If the Security Investigation Type block has the code "U", or is blank, request clearance action "I" on TTC 040.

b. DONCAF may be called at DSN 288-8880/1/2/3/4 to verify clearance eligibility, investigative basis, and completion dates, but no more than three inquiries are allowed per call.

11004. INVESTIGATIVE REQUIREMENTS FOR ACCESS TO NATO INFORMATION

The investigative basis for the U.S. clearance (favorably adjudicated SSBI, PR, NAC or NACI, depending on the NATO access the billet requires) must have been completed within the last five years. Continued assignment to a NATO COSMIC Top Secret billet requires a PR every five years. Submit PR requests to Navy Liaison Office, P. O. Box 1211, Baltimore, MD 21203. For NATO Secret, a new NAC is required every five years.

11005. PERIODIC REINVESTIGATIONS. An individual who has been previously investigated under the provisions of the reference will be re-investigated periodically (once every five years) only under the conditions outlined in paragraph 21-2 of the reference.

11006. REQUESTS FOR PERSONNEL SECURITY INVESTIGATIONS

1. Security Managers are responsible for requesting PSI's on assigned personnel, with the exception of those personnel requiring access to SCI. PSI's for SCI access will be forwarded to the MARRESFOR SSO for processing.

required to maintain a minimum continuous security clearance eligibility.

11003. INVESTIGATIVE REQUIREMENTS FOR PERSONNEL SECURITY CLEARANCE

1. The Headquarters Battalion Security Manager and unit Security Managers will ensure that all personnel have the appropriate security investigation and that this information is entered into the Joint Uniform Military Pay System (JUMPS) or the Reserve Manpower Pay System (REMMPS).
2. All Navy and Marine Corps enlisted personnel below the rank of SSgt shall have at least an Entrance National Agency Check (ENTNAC). The primary reason for an ENTNAC is to determine an individual's suitability for entry into the armed forces.
3. All Navy and Marine Corps officers and all SNCO's shall have at least a National Agency Check (NAC) with a completion date no older than 10 years. Officers and SNCO's with investigations older than 10 years should resubmit the appropriate investigation forms for eligibility up to the level of Secret.
4. The investigative requirement for a final Top Secret security clearance is the Single Scope Background Investigation (SSBI). All SSBI's will be updated once every five years by Periodic Reinvestigation (SSBI-PR).
5. The investigative requirement for a final Secret or Confidential clearance is the ENTNAC or the NAC.
6. Investigation requirements for performance of specific duties (Non SCI) are as follows:
 - a. All officers and staff non-commissioned officers in the communications field shall have an SSBI completed or updated within the last five years.
 - b. All personnel in MOS 57XX shall have at least a NAC completed or updated within the last five years.
 - c. All Top Secret Control Officers and their assistants shall have an SSBI completed within the last five years.
 - d. All Security Managers shall have an SSBI completed or updated within the last five years.
 - e. Commanding Officers, Executive Officers and Operations Officers of Battalions/Squadrons or higher shall have an SSBI completed or updated within the last five years.

9. Security Managers will be guided in their duties and responsibilities by the reference and this Manual.

11001. BASIC POLICY

1. No person will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made in regard to loyalty, reliability and trustworthiness. The initial determination will be based on a local records check and on a personnel security investigation (PSI) appropriate to the level of access required.
2. Requests for PSI's must be kept to an absolute minimum. Investigations will not be requested to resolve allegations of a suitability nature for the purpose of supporting personnel administrative decisions or disciplinary procedures independent of a personnel security determination.
3. The Defense Investigative Service Personnel Investigations Center (DIS/PIC) conduct all GENSER level PSI's for Department of the Navy personnel.
4. All investigative requests, except for SCI access, will be mailed directly to DIS/PIC. The results will be forwarded to Director, Department of the Navy, Central Adjudication Facility (DONCAF).
5. All Navy and Marine Corps enlisted personnel shall have at least an Entrance National Agency Check (ENTNAC). If DONCAF has no record of an ENTNAC on file for any enlisted individual, the Security Manager will submit a National Agency Check (NAC) on the subject individual after the need for a PSI has been identified.

11002. CLEARANCE ELIGIBILITY AND CRITERIA

1. Only U.S. citizens (Native or Naturalized) are eligible for a security clearance. A security clearance for access to classified information or equipment will be based on the PSI prescribed for the level of classification necessary to accomplish assigned duties.
2. Paragraph 21-5, of the reference requires that personnel in certain MOS' be eligible for a security clearance and be U.S. citizen. DON personnel who are non U.S citizens and/or are not eligible for a security clearance for personnel security reasons will not be allowed into or remain in the listed MOS'. MCO 5521.3H (Personnel Security Investigations, Security Clearances, and Access) also lists MOS' in which personnel are

SOP FOR ISP

CHAPTER 11

PERSONNEL SECURITY INVESTIGATION, CLEARANCE, AND ACCESS PROGRAM

11000. GENERAL

1. The MARRESFOR Security Manager (MARRESFOR SecMgr) has overall responsibility for the Information Security Program (ISP) and will provide guidance and direction to major supporting commands, and subordinate/attached units.
2. The Headquarters Battalion Security Manager is responsible for administering personnel security requirements for personnel assigned to Headquarters Battalion, MARRESFOR (HQ MARRESFOR). This includes Active Duty Marines of the 4th MarDiv, 4th MAW, 4th FSSG and reserve personnel attached to or under the cognizance of the MARRESFOR Headquarters.
3. The 2d and 3d MEB Security Managers are responsible for administering personnel security requirements for active and Reserve personnel assigned to them.
4. The 4th MarDiv Security Manager is responsible for the administration of personnel security requirements for Reserve personnel assigned to or under the cognizance of the 4th MarDiv Headquarters, and is the immediate superior in command for security issues for subordinate units.
5. The 4th MAW Security Manager is responsible for the administration of personnel security requirements for Reserve personnel assigned to or under the cognizance of the 4th MAW Headquarters, and is the immediate superior in command for security issues for subordinate units.
6. The 4th FSSG Security Manager is responsible for the administration of personnel security requirements for Reserve personnel assigned to or under the cognizance of the 4th FSSG Headquarters, and is the immediate superior in command for security issues for subordinate units.
7. The MCRSC Security Manager is responsible for the administration of personnel security requirements for Active Duty and Reserve personnel assigned to or under the cognizance of the MCRSC Headquarters, and is the immediate superior in command for security issues for Individual Ready Reserve (IRR) personnel.
8. Subordinate unit Security Managers are responsible for all personnel assigned to their unit(s).

SOP FOR ISP

	PARAGRAPH	PAGE
DENIAL/WITHDRAWAL OF SECURITY CLEARANCE FOR CAUSE	11019	11-14
TERMINATION OF ACCESS	11020	11-15
VISITOR AUTHORIZATION REQUESTS	11021	11-15
INVESTIGATION REQUIREMENTS FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION (SCI)	11022	11-15
MOBILIZATION AND SCI ACCESS	11023	11-16

FIGURES

11-1	PERSONNEL SECURITY ACTION REQUEST	11-17
11-2	REQUEST FOR ACCESS TO CLASSIFIED INFORMATION	11-18
11-3	REQUEST FOR JUMPS/REMMPS/MMS ENTRY	11-19
11-4	REQUEST FOR CLEARANCE/ACCESS TO CLASSIFIED MATERIAL	11-20
11-5	SINGLE SCOPE BACKGROUND INVESTIGATIONS SUBMISSION PROCEDURES	11-21

SOP FOR ISP

CHAPTER 11

PERSONNEL SECURITY INVESTIGATION, CLEARANCE, AND ACCESS PROGRAM

	PARAGRAPH	PAGE
GENERAL	1100	11-3
BASIC POLICY	11001	11-4
CLEARANCE ELIGIBILITY AND CRITERIA . . .	11002	11-4
INVESTIGATIVE REQUIREMENTS FOR PERSONNEL SECURITY CLEARANCE	11003	11-5
INVESTIGATIVE REQUIREMENTS FOR ACCESS TO NATO INFORMATION	11004	11-6
PERIODIC REINVESTIGATIONS	11005	11-6
REQUESTS FOR PERSONNEL SECURITY INVESTIGATIONS	11006	11-7
PREPARATION AND SUBMISSION OF INVESTIGATIVE REQUESTS.	11007	11-8
REPORTS OF INVESTIGATION	11008	11-8
REQUESTS FOR ADDITIONAL INFORMATION . . .	11009	11-9
GRANTING CLEARANCES	11010	11-9
INTERIM AND FINAL CLEARANCES	11011	11-10
NATO SECURITY CLEARANCE	11012	11-10
NAVAL WARFARE PUBLICATIONS (NWP) SECURITY CLEARANCE	11013	11-10
ACCESS	11014	11-11
REQUESTING AND GRANTING CLEARANCES . . .	11015	11-12
ONE-TIME ACCESS	11016	11-12
ACCESS BY RESERVE PERSONNEL	11017	11-13
SUSPENSION OF ACCESS.	11018	11-13

10006

SOP FOR ISP

f. Provisions have been made to control and safeguard classified material given to those attending and to retrieve the material or effect transfer of control through approved methods.

g. Sessions are monitored to ensure discussions are limited to the level authorized.

and (as available) nationality, title, office and sponsor of the visitor, clearing authority if the visit includes disclosure of classified information, the date and duration of the visit and the name of the escort, if used. These records will be retained for two years.

10006. MEETINGS

1. Basic Policy. In this Manual, meetings are defined as a gathering of personnel for the purpose of discussing or presenting information. Classified information will not be disclosed at conferences, symposia or other gatherings (hereafter called meetings) unless disclosure of the information serves a Government purpose and adequate security measures are taken to control access to the information and prevent its compromise.
2. A meeting conducted or sponsored by this Headquarters or subordinate units at which classified information is to be disclosed, must comply with chapter 19 of the reference.
3. Units must receive written permission from their higher headquarters (Security Manager) to hold a meeting in which classified information is to be disclosed.
4. The unit conducting a classified meeting, will be the security sponsor and be responsible for ensuring that the following security requirements are met:
 - a. Areas in which classified information is to be discussed afford adequate security against unauthorized access.
 - b. Adequate storage facilities are available.
 - c. Each person attending has been authorized access to information of equal or higher classification than the information being disclosed.
 - d. Admittance is limited only to those on an approved access list and then only upon proper identification.
 - e. Each person who will disclose classified information has been notified of the security limitations which must be imposed because of:
 - (1) The level of access authorized for all attendees.
 - (2) Need to know of attendees; and
 - (3) Physical security conditions.

access required.

f. Security clearance status of visitor (basis of clearance is not required).

g. Where appropriate, names of persons to be visited.

2. Requests will be submitted in advance of the proposed visit in sufficient time to permit processing and to make a determination as to whether or not the visitor should or will be granted access.

3. Visitors who are authorized access to classified information will present adequate identification at the time of their visit.

4. The Security Manager will maintain a file of all visit requests for a period of two years. A copy of the visit request will be provided to the member/section being visited.

5. Personnel from the MARRESFOR Headquarters visiting other commands will submit visit requests in advance of the proposed visit, in sufficient time to permit processing and to make a determination as to whether or not the visitor should or will be granted access.

10004. VISITS BY FLAG GRADE OFFICERS AND THEIR CIVILIAN EQUIVALENTS. As a matter of courtesy, flag grade officers and their civilian equivalents will not be required to sign visitor records or display identification badges when being escorted as visitors. Identification of these senior visitors by their escorts will be sufficient.

10005. VISITS BY FOREIGN NATIONALS

1. Visits by foreign nationals which will involve technical discussions or the disclosure of classified information require the approval of the Commandant of the Marine Corps. Policy and procedures for visits of nationals from designated countries are contained in OPNAVINST C5510.159. In general, a U.S. commander, when he/she feels it to be in the best interests of the United States, may invite or permit foreign nationals to visit his/her command on courtesy calls and for general visiting.

2. Except during general visiting, a record of all visits to this Headquarters and subordinate commands by foreign nationals, or by U.S. citizens or immigrant aliens representing foreign governments, military services or private interest will be maintained. The record will consist of the name of the visitor

SOP FOR ISP

CHAPTER 10

VISITOR CONTROL AND MEETINGS

10000. GENERAL. A visitor is any person who is not attached to or employed by MARRESFOR. This chapter provides guidance for visitor control procedures, classified conferences and exercises.

10001. VISITOR CONTROL OFFICER. The Commanding General, MARRESFOR has the overall responsibility for visitor control within MARRESFOR. This authority is delegated to the MARRESFOR Security Manager, and subordinate command Security Managers. The Commanding Officer, Headquarters Battalion and MARRESFOR General and Special staff officers will follow the visitor control procedures outlined in ForO P5000.1. Subordinate commands will be responsible for establishing visitor control procedures within their respective commands.

10002. GENERAL VISITING. All general visiting, such as tours of MARRESFOR Headquarters spaces or facilities, will be on an unclassified basis and coordinated through the Public Affairs Office, MARRESFOR and per ForO P5000.1. General visits to subordinate commands will be coordinated through the respective unit.

10003. CLASSIFIED VISITS. Any visit involving access to classified information requires the commanding officer of the visitor, or an appropriate official of the contractor facility, organization or foreign country which the visitor represents, to submit a visit request to the commanding officer of the command to be visited.

1. Visit requests must include the following information:

a. Name in full, rank, rate, or grade (when applicable), title, position, and citizenship of the proposed visitor. If an immigrant alien, so indicate.

b. Employer or sponsor, if other than the originator of the request.

c. Name and address of the activity to be visited, if other than the addressee of the visit request.

d. Date, time and duration of the proposed visit.

e. Purpose of visit in detail, including estimated degree of

SOP FOR ISP

CHAPTER 10

VISITOR CONTROL AND MEETINGS

	PARAGRAPH	PAGE
GENERAL	10000	10-3
VISITOR CONTROL OFFICER	10001	10-3
GENERAL VISITING	10002	10-3
CLASSIFIED VISITS	10003	10-3
VISITS BY FLAG GRADE OFFICERS AND THEIR CIVILIAN EQUIVALENTS	10004	10-4
VISITS BY FOREIGN NATIONALS	10005	10-4
MEETINGS	10006	10-5

been designated as restricted.

9008. TELECOPIERS. Telecopiers, facsimile equipment or similar devices will not be used to reproduce classified information without prior approval from the cognizant Security Manager.

to any restrictions imposed for the protection of classified material.

3. Photographic equipment will not be taken into the Sensitive Compartmented Information Facility (SCIF).

9006. PHOTOGRAPHS BY COMMERCIAL PHOTOGRAPHERS

1. All photographs will be submitted to the MARRESFOR Commanding General or the appropriate Security Manager for review. If photographs are determined to be classified, a suitable classification will be assigned and they will be forwarded up the chain of command, with all negatives and copies, to the Special Assistant for Public Affairs Support (OP-09C), via Headquarters, U.S. Marine Corps (ARAD).

2. All commercial negatives and prints will remain under Department of the Navy jurisdiction until officially released (see Chapter 8 of SECNAVINST 5720.44A).

3. Civilian photographers will be informed that the retention of negatives and prints, or the publishing of photographs in violation of their agreement, or failure to deliver negatives or prints to proper authority upon demand may render them liable to prosecution under the espionage act (18 U.S.C. 792-799).

4. In the mutual interest of the Department of the Navy and organizations engaged in photographic work, whenever a civilian photographer is authorized to take pictures ("still", motion picture or videotape), the Security Manager in coordination with the Public Affairs Officer will act in an advisory capacity to the photographer to prevent inadvertent disclosure of classified material.

5. When supervision of photography has been such as to preclude the inclusion of subjects prohibited for release, the official granting permission to take these pictures may release them immediately for publication without prior inspection of the prints or negatives.

9007. CONTROL OF RECORDING SYSTEMS

1. Personnel will be allowed to bring voice recording equipment only when authorized by the Section Heads of the General and Special Staff Sections subject to any restrictions imposed for the protection of classified information.

2. Audiovisual equipment is not allowed in the Sensitive Compartmented Information Facility (SCIF) or any area that has

be checked for classified material that may have been left or thrown in wastebaskets. If a machine malfunctions, it will be checked to ensure that all copies have been removed.

6. Reproduced copies of documents can leave legible images on the plastic surfaces of many binders after the paper and plastic have been in contact for a period of time. All classified documents will use classified document cover sheets to preclude transferring any image to the cover of plastic binders.

9004. PHOTOGRAPHY CONTROLS

1. The MARRESFOR Security Manager in coordination with the Public Affairs Officer has overall responsibility for controlling photography and ensuring appropriate security guidelines and provisions are followed for the MARRESFOR Headquarters and other USMC units located at the Hebert Defense Facility, New Orleans. Subordinate unit security managers, in coordination with the Commander of their host facilities, are responsible for their respective units and sites.

2. Visitors to MARRESFOR units and sites may be authorized to take photographs. The visitor will be escorted by a member of the command to ensure no classified or sensitive material is photographed.

3. Care must be taken to protect classified material from compromise through photography. Remove or cover classified material within the range of the camera.

4. Classified photographs and negatives will be marked per Chapter 9 of the rence and safeguarded as prescribed for other material of the same classification.

5. When using self-processing film or paper to photograph classified material, (Polaroid type) the negative of the last exposure will be removed and destroyed as classified waste, or protect the camera as classified material.

9005. PHOTOGRAPHS BY DOD/NAVY/USMC PERSONNEL

1. Marine Corps Public Affairs personnel and Training Audio/Visual Support Unit personnel are authorized to act as official photographers for the command. Developing and printing is under Department of the Navy jurisdiction.

2. Marine Corps Public Affairs personnel authorized by the Commanding General to bring cameras into the command are subject

4. Machines that are not authorized for reproduction of classified material will be posted with the following notice: "REPRODUCTION OF CLASSIFIED MATERIAL NOT AUTHORIZED ON THIS MACHINE."

5. Equipment for reproduction of Top Secret material will be located only in the MARRESFOR CMCC or Sensitive Compartmented Information Facility.

9003. REPRODUCTION CONTROLS

1. Top Secret. Sections requiring reproduction of Top Secret material will submit a written request to the Top Secret Control Officer (TSCO).

a. The TSCO will initiate action to obtain reproduction approval from the document originator.

b. Once approval is obtained, the TSCO will accomplish the reproduction. The TSCO will ensure two Top Secret (TS) cleared personnel perform the reproduction. When reproduction is accomplished, the TSCO will log in, mark, and control all copies.

c. The TSCO will retain Top Secret document reproduction records (approval letters, logs, etc.) for two years.

2. Secret and Confidential. The OIC, CMCC has the cognizance for reproduction authority for controlled Secret and Confidential Material. Sections requiring reproduction of Secret and Confidential documents controlled by MARRESFOR will submit a written request to the OIC, CMCC. Once reproduction is accomplished, the OIC, CMCC will log in, buck-tag, and control all copies. Non bucktagged Secret and Confidential material will be authorized for reproduction by the Section Head holding the material.

3. Non bucktagged classified material will be reproduced on authorized reproduction machines only. Only classified material controlled by the CMCC may be transmitted outside the command.

4. Reproduced material must show the classification and other special markings which appear on the original material, and will be afforded the same security controls as those required for the original document.

5. Security Precautions. Any samples, wasted or overruns will be safeguarded based on the classification of the information contained thereon. This material will be promptly destroyed as classified waste. Areas surrounding reproduction equipment will

SOP FOR ISP

CHAPTER 9

REPRODUCTION AND PHOTOGRAPHY OF CLASSIFIED MATERIAL

9000. GENERAL. Commanding Officers are responsible for all reproduction and distribution of classified material within their commands. The term "reproduction" will include reproduction machines, i.e., XEROX type machines, etc., photography, television, audio and visual recording equipment, artists, sketches and draftsmen, telecopiers and facsimile machines (FAX machines), or any other medium able to record and store images or data. It is the policy of this command that reproduction of classified material will occur only when absolutely necessary and then only when specifically authorized as detailed below.

9001. REPRODUCTION AUTHORITY

1. Top secret material will not be approved for reproduction without written approval by the originator.
2. Secret and Confidential material that is controlled and has been assigned a buck-tag number by the CMCC will be reproduced only by the OIC, CMCC or his designate.
3. Secret and Confidential material that is uncontrolled (not bucktagged) will be authorized for reproduction only by the Section Head holding the material or his designate.

9002. REPRODUCTION EQUIPMENT

1. A reproduction machine designated for classified material reproduction will be located in an area where reproduction can be controlled and precautions taken to prevent viewing of the material by unauthorized personnel.
2. A sign will be located on or near the reproduction machine which states "THIS MACHINE MAY BE USED FOR REPRODUCTION OF CLASSIFIED MATERIAL UP TO AND INCLUDING SECRET. REPRODUCTION MUST BE APPROVED BY OIC, CMCC OR SECTION HEAD."
3. Upon completion of the reproduction of classified material, personnel will place a blank sheet of paper on the machine and reproduce it no fewer than three times. This will help ensure that no images are left on the machine. If a malfunction or paper jam occurs during reproduction of classified material extreme care should be taken to ensure that classified material is not left in the paper path.

SOP FOR ISP

CHAPTER 9

REPRODUCTION AND PHOTOGRAPHY OF CLASSIFIED MATERIAL

	PARAGRAPH	PAGE
GENERAL	9000	9-3
REPRODUCTION AUTHORITY	9001	9-3
REPRODUCTION EQUIPMENT	9002	9-3
REPRODUCTION CONTROLS	9003	9-4
PHOTOGRAPHY CONTROLS	9004	9-5
PHOTOGRAPHS BY DOD/NAVY/USMC PERSONNEL . .	9005	9-5
PHOTOGRAPHS BY COMMERCIAL PHOTOGRAPHERS . .	9006	9-6
CONTROL OF RECORDING SYSTEMS	9007	9-6
TELECOPIERS	9008	9-7

specific situation germane to each section. It will be located near the entrance/exit to all vaults, strong rooms, or offices used for the storage of classified materials (restricted areas).

c. Security Container Check Sheet (SF 702). The SF 702 will be placed on all security containers containing classified materials and on the outside of hatches to vaults and strong rooms. It is a record of inspection to ensure vaults, strong rooms and security containers are secured each day.

d. Security Cover Sheet Top Secret (SF 703), Security Cover Sheet Secret (SF 704), Security Cover Sheet Confidential (SF 705). The appropriate cover sheet will be used and placed over classified material whenever it is removed from a security container.

e. Security Container Record Form (OPNAV 5510/21). OPNAV 5510/21 will be maintained in the control drawer of the security container. All repairs and modifications to the security container will be annotated on this form.

2. Emergency Notification. A list will be posted in each repository drawer of each security container identifying individuals to contact in the event the security container is found unsecured. The Security Container Information Form (SF 700) may be used.

8008. REPAIRS AND MODIFICATIONS TO SECURITY CONTAINERS

1. Neutralization of lockouts or repair of any damage which affects the integrity of a container approved for storage of classified material will only be done by appropriately cleared or continuously escorted personnel specifically trained in the approved methods. Notify the local Security Manager when any lockout or repair is required.
2. Security Managers that are required to have repairs or modifications performed on security containers will utilize repair personnel that have been cleared and are under contract to GSA, if available. The Security Manager will contact the local GSA office for the names of such personnel. If GSA does not have contracted repair personnel, the Security Manager may attempt to contact other security agencies, i.e., military units (Army MI, Air Force OSI, etc.), local security agencies (the FBI, the State Bureau of Investigation, SBI, etc.) or law enforcement agencies for advice on local cleared contract locksmith personnel. Security considerations must be foremost at all times during repairs and modifications to security containers.
3. External modifications of GSA approved security containers to attach additional locking devices, alarms, etc., is authorized as long as the modification does not affect the security integrity of the container. All modifications will be entered on the OPNAV Form 5510/21.
4. All requests for security container repair, lookout, combination change, etc., for container located at the Hebert Defense Complex must be approved by the MARRESFOR Security Manager prior to a Purchase Order being approved.

8009. SECURITY FORMS

1. The following security related forms will be utilized.
 - a. Security Container Information Form (SF 700). The SF 700 is a record for each vault, strong room or security container storing classified material. It will be maintained showing the location of the container, the names, home addresses, and home telephone numbers of persons having knowledge of the combination. It is maintained inside the control drawer of security containers and on the inside of the hatch to vaults and strong rooms.
 - b. Activity Security Checklist (SF 701). The SF 701 is used to denote security checks of working areas upon securing for the day. It contains blank areas to be annotated to reflect the

j. If combinations are transmitted outside of the command all applicable provisions of chapter 5 of this Manual must be adhered to.

k. CMS combinations may be stored in appropriate security containers if each combination is placed in separate, sealed security container information forms (SF 700). The outside of the sealed form will contain the name, rank, home address, and telephone number of all persons having knowledge of the combination.

l. Combinations will not be changed by personnel not having the appropriate security clearance.

4. Supplemental Locks and Access Control

a. Security Padlocks. The only approved padlocks for use in conjunction with securing classified material and equipment are Sargent and Greenleaf's #8065 and #8077A locks.

b. STU-III Ignition Keys (CIK). Keys will not be left in the units overnight. CIK's will be removed from and secured away from the STU-III when not in use. CIK's are not required to be secured in a GSA container.

c. Electrical and Mechanical Locks. Cypher and Simplex locks do not afford the degree of protection required for classified information. They will not be used as the primary means to safeguard classified material. However, such locks are authorized as traffic control devices for restricted areas.

d. Intrusion Detection Systems (IDS). Intrusion detection systems provide a means of detecting and announcing proximity or intrusion which endangers or may endanger the security of the command. Because of their cost, IDS are justified only where their use results in a commensurate reduction or replacement of other protective elements without loss of protective effectiveness. Questions concerning requirements for IDS should be addressed to the MARRESFOR Security Manager.

8007. SECURING SECURITY CONTAINERS. The dial of combination locks will be rotated at least four complete turns in the same direction when securing containers or doors. With most locks, if the dials are given only a quick twist, it is possible to open the lock merely by turning the dial back in the opposite direction. Each drawer of the containers will be checked to ensure they are fully secured.

whose official duties demand access to the container.

b. Combinations will be changed when any of the following instances occur:

- (1) At least annually;
- (2) When containers and locks are first placed into use;
- (3) When an individual knowing the combination no longer requires access;
- (4) When the combination has been subject to possible compromise or the security container has been discovered unlocked or unattended;
- (5) When the security container (with built-in lock) or the padlock is taken out of service.

c. Built-in combination locks will be reset to the standard 50-25-50. Combination padlocks will be reset to the standard combination 10-20-30.

d. In selecting combination numbers, sequential numbers (i.e., multiples of 5, simple ascending or descending arithmetical series) and personal data, such as birth dates and Social Security Numbers will not be used.

e. The same combination will not be used for more than one container in any one classified material storage area.

f. In setting a combination, numbers should be used that are widely separated by dividing the dial into three parts and using a number from each third as one of the combination numbers.

g. To prevent a lockout, two different people should try the new combination at least three times before closing the container or vault door.

h. The combination of a vault or security container will be assigned a security classification equal to the highest category of the classified material authorized to be stored therein.

i. Records of combinations will be annotated and sealed in the Security Container Information Form, SF 700. The SF 700's will be kept at the next echelon of command's CMCC (e.g., combination to company's security containers at its battalion, squadron's combination at the group, etc.). Combinations may be stored at host command communications centers if desired. Combinations for all security containers at the MARRESFOR Headquarters will be kept in the CMCC.

storage of classified material. This form will be placed inside the control drawer of each container. The containers will be inspected periodically. Inspections and repairs will be annotated on the form.

c. Each security container used for the storage of classified material will have a current properly completed Security Container Information Form (SF 700) attached to the inside of the control drawer.

d. Valuables, such as money, jewels, precious metals, narcotics, or weapons/ammunition, will not be stored in the same container used to safeguard classified material. These items increase the risk of a container being opened or stolen, with the resulting compromise of the information therein.

e. For identification purposes in the event of emergency action, a number, letter, or other symbol will be placed on the exterior of each security container that represents the priority for evacuation or destruction of the material. The exterior marking will not indicate the level of classified information stored in the container.

f. Safes and security containers that are not being utilized for storage of classified material will have a sign attached to it which reads, "THIS CONTAINER IS NOT USED FOR THE STORAGE OF CLASSIFIED MATERIAL."

g. CMS Material will be stored in Two-Person-Integrity (TPI) modified GSA approved security containers.

h. When alarms are used to enhance security, the physical barrier must be adequate to prevent surreptitious removal or observation that would result in the compromise of the material. The physical barrier must be such that forcible attack will result in evidence of attempted entry into the room or area. The alarm system must, at a minimum, provide immediate notice to the Duty Officer and/or security force of an attempted entry.

2. Vaults and Strong rooms. Storage requirements for large amounts of classified material, or odd-shaped or bulky material, can be met in many instances by vaults or strong rooms. They must conform and be built to the standards specified in the reference, Exhibit 14B. Vaults or strong rooms may not be used for storage of classified material unless a current PSE has been conducted.

3. Combination Locks. To ensure the effectiveness of combination locks, the following requirements apply:

a. The combination will be given only to those personnel

be permitted to work alone in areas where Top Secret or other information requiring TPI is used or stored. TPI will be strictly adhered to outside of normal working hours. The TPI requirement for WWMCCS terminals is usually waived annually by message from JCS.

5. Security Checks

a. Section heads will require a security check of each office and working space at the end of each working day to make sure all classified material is properly secured. Standard Form (SF) 701, Activity Security Checklist will be used to record such checks. SF 701 will be posted near the entrance of every restricted area that processes or stores classified material.

b. An integral part of the security check system consists of securing all strong rooms, vaults, and security containers used for the storage of classified material. Standard Form 702, Security Container Check Sheets will be posted on the outside of each security container and used to record such actions. SF 702 will be completed by the SCPC or designate having cognizance over that security container. Standard Forms 701 and 702 will be used to reflect after hours, weekends and holidays activities.

c. Personnel will ensure that all classified material is properly secured, burn bags are properly stored, all classified notes, rough drafts, carbon paper, classified typewriter and printer ribbons and similar items have been properly stored or destroyed. Strong rooms, vaults and security containers will be locked by the responsible custodians and double checked. (The dial of the combination locks MUST be rotated at least four complete times in the same direction when securing safes, files and cabinets.)

8006. STORAGE REQUIREMENTS

1. Security Containers. Only General Service Administration (GSA) approved security containers will be utilized for the storage of classified material and equipment. GSA approved field safes or portable containers, if utilized, will be rendered non-portable by securing them to a permanent fixture while in a garrison environment. While in the field, field safes will be safeguarded by appropriate personnel and never left unattended.

a. The best security container in the command will be used for the storage of the most sensitive material.

b. A Security Container Records Form (OPNAV Form 5510/21) will be maintained for each security container used for the

2. Work Spaces

a. All sections, sites and units will implement the security measures necessary to prevent unauthorized persons from gaining access to classified material, including security measures to prevent personnel outside the building and spaces from viewing or overhearing classified material and discussions.

b. In providing these measures, the following precautions will be taken: Ground floor windows or other accessible openings should be equipped with barriers, i.e., heavy grills, screens or bars which defeat access from the outside; windows should be opaque or be fitted with curtains or blinds to prevent visual access.

c. Contract maintenance and cleaning personnel requiring access to areas and offices working with classified information will be escorted at all times.

d. Extraneous material (such as unclassified papers, ADP printouts) will be kept off the tops of security containers to prevent inadvertent mingling of classified with unclassified materials.

e. Personal radios, TV's, or recording devices will not be allowed in classified discussion areas.

3. Care During Working Hours. During working hours the following precautions will be taken to prevent either visual or audible access to classified information by unauthorized personnel:

a. When classified material is removed from the security container, it will be kept under constant surveillance by appropriately cleared personnel. An appropriate cover sheet (SF 703, 704, 705), will be placed over all classified material to prevent visual access. When not in use the material will be returned to an approved security container for safeguarding.

b. Classified material will not be left unattended for any reason.

c. Items containing classified information, such as carbon and plastic typewriter/printer ribbons, carbons, work sheets, etc., will be protected in the same manner as prescribed for the highest level of classified material they contain. After use, such items will either be properly destroyed or secured in an approved security container.

4. Two-Person Integrity Requirement (TPI). Personnel will not

mission sensitivity, arms, ammunition and explosives, or items having a high likelihood of theft. There are three types of Restricted Areas.

(1) Level Three. The most secure type of Restricted Area contains a security interest which would cause grave damage to national security if lost, stolen or compromised. Access to this level constitutes actual access to the security interest or asset. It is a clearly defined protected area, incorporates a personnel identification and control system, and includes an access list and entry and departure log. Admission is only to those persons who have been granted appropriate authorization. A SCIF or an Armory are examples of a Level Three Restricted Area.

(2) Level Two. This area contains security interests which could cause serious damage to national security if lost, stolen or compromised. Uncontrolled or unescorted movement could permit access to the security interest. It is a clearly defined area and incorporates personnel identification and control systems. During normal working hours an access list and entry and departure log is suggested but not required. Admission is only to those persons whose duties require access and have the appropriate authorization. A Command Operations Center, Intelligence Operations office, or any area that has open storage of classified material (such as a vault or strong room) are examples of Level Two Restricted Areas.

(3) Level One. This area contains a security interest which could cause damage to national security if lost, stolen or compromised. Uncontrolled movement may or may not permit access to the security interest. It is a clearly defined area that incorporates personnel identification and control systems. Ingress and egress is controlled. Military Reservations or unit compounds are examples of Level One Restricted Areas. All work spaces where classified information is stored are designated as Level One Restricted Areas.

b. Signs and Postings

(1) Signs to restricted Areas will read as follows:

WARNING

RESTRICTED AREA - KEEP OUT

AUTHORIZED PERSONNEL ONLY

(2) All words except "WARNING" will be black. The word "WARNING" will be red. All wording will be on red, white or blue backgrounds, to obtain maximum color contrast.

4. Should the results of the PSE indicate that significant changes or modifications to the facility are required, it will be the local Security Manager's responsibility to implement corrective action and resubmit the request for another PSE when modifications are completed. Classified material will not be stored at any unit if proper storage facilities or equipment is not in place.

5. A new PSE or certification letter will be requested when:

a. There is a significant physical modification of the vault or strong room.

b. The repository has been moved to a different office or building.

8004. CHAPTER 14 REVIEW

1. A Chapter 14 Review is a review and validation of the physical security and storage criteria established for classified material in Chapter 14 of OPNAVINST 5510.1H. It replaces PSE's for classified material storage areas that do not require open storage of the material. Units that do not have vaults or strong rooms will replace PSE's with the Chapter 14 Review.

2. Prior to requesting authority to establish a SCP, the unit will conduct a security review of their existing classified material storage area using Chapter 14 of the reference.

3. When the unit/site meets all the criteria for storage of classified material, they will indicate it as part of their request for an Establishment of an SCP Letter (see figure 6-7).

4. The Chapter 14 Review paperwork will be maintained by the unit conducting the review and does not have to be sent to MARRESFOR Headquarters.

5. CMS storage requirements are regulated by the CMS41 and CSP1A

8005. SECURITY REQUIREMENTS

1. Restricted Areas

a. Different areas require higher degrees of security due to the nature of the work, information and material concerned. Such areas will be designated only as RESTRICTED AREAS. They will be posted with warning signs at all points of ingress and egress. While safeguarding classified material is a basic function, other valid reasons exist to establish Restricted Areas. These include

without specific approval of the Commanding General, MARRESFOR. Approval will be given only when there is an overriding need, the required physical safeguards, including a GSA-approved storage container, are provided, and a list of the material removed is kept at the command. Approval to remove classified material will not include permission for overnight storage in any location other than a secure U.S. Government facility.

8002. AUTHORIZATION TO STOW. Classified material and equipment will only be maintained in those areas or spaces that have been specifically approved and authorized in writing by the unit Security Manager. MARRESFOR Headquarters area unit and sections will submit requests to the MARRESFOR OIC, CMCC. This approval will be in writing, and based upon a satisfactorily completed Physical Security Evaluation (PSE) or Chapter 14 Review (OPNAVINST 5510.1H) of the facility. Requests for the establishment of Secondary Control Points for storage of classified material will be addressed to the OIC, CMCC for action. (See paragraph 6011 and figure 6-7).

8003. PHYSICAL SECURITY EVALUATION (PSE)

1. A formal Physical Security Evaluation (PSE) will be performed on vaults and strong rooms only. PSE's will be conducted by qualified personnel designated or approved by the MARRESFOR Security Manager. A copy of the completed PSE will be forwarded to the Unit Commander or the MARRESFOR Security Manager. This document can be used by the unit Security Manager to authorize storage of classified material (up to the level specified in the PSE) as long as all recommendations have been met and all other security considerations are recognized. Copies of the PSE will be maintained by the CMCC and the SCP having cognizance over the material.

2. Storage of classified material marked Secret or Confidential NOT in an approved vault or strong room must be stored in a GSA approved security container. All other applicable requirements of the reference must also be met. For subordinate units not located at the MARRESFOR Headquarters, New Orleans, the Unit Commander will conduct a Chapter 14 Review then certify in writing that the classified material storage facilities at that site meets the requirements of the reference.

3. The PSE Report and Unit Commander Chapter 14 Review Certification will be kept on file by the local Security Manager until that unit no longer stores classified material. The MARRESFOR Security Manager and the OIC, CMCC will maintain copies of all PSE's and Chapter 14 Reviews conducted on sections within the MARRESFOR Headquarters.

SOP FOR ISP

CHAPTER 8

SECURITY AND STORAGE OF CLASSIFIED MATERIAL

8000. GENERAL

1. Section Heads are responsible for the security, safeguarding and storage of classified material within their sections. They will adhere to the policies and procedures set forth in this Manual. Classified information or material will only be used where there are adequate facilities to prevent unauthorized persons from gaining access to it. They will ensure that classified information which is neither being used nor under the personal observation of cleared personnel, who are authorized access, is safeguarded and stored as prescribed by this Manual. Specific security requirements will depend on the conditions within each section. The requirements specified in this Manual represent the minimum acceptable standards. Any weakness or deficiency in safeguarding and storage procedures will be immediately identified to the Security Manager.

2. Security and storage requirements were developed to provide a uniform guide for establishing security protection for classified material and equipment, commensurate with the security interest in the material or equipment. Storage requirements must be tempered and balanced by common sense and security-in-depth. (Security-in-depth: overlapping or reinforcing measures incorporated in such a manner that failure of one security measure will not expose the protected material or equipment to compromise.)

8001. SECURITY AND STORAGE REQUIREMENTS

1. Anyone who has possession of classified material is responsible for safeguarding it at all times and particularly for securing classified material in appropriate security containers whenever it is not in use. The custodian must follow procedures which ensure that unauthorized personnel do not gain access to classified information by sight or sound or other means. Classified information will not be discussed with or in the presence of unauthorized personnel.

2. Personnel will not remove classified material from designated office or working areas except in performance of official duties and under conditions providing protection required by this Manual. Under no circumstances will personnel remove classified material from designated areas to work on it during off duty hours, or for any other purpose involving personal convenience,

SOP FOR ISP

CHAPTER 8

SECURITY AND STORAGE OF CLASSIFIED MATERIAL

	PARAGRAPH	PAGE
GENERAL	8000	8-3
SECURITY AND STORAGE REQUIREMENTS	8001	8-3
AUTHORIZATION TO STOW	8002	8-4
PHYSICAL SECURITY EVALUATION (PSE) . . .	8003	8-4
CHAPTER 14 REVIEW	8004	8-5
SECURITY REQUIREMENTS	8005	8-5
STORAGE REQUIREMENTS	8006	8-8
SECURING SECURITY CONTAINERS	8007	8-11
REPAIRS AND MODIFICATIONS TO SECURITY CONTAINERS	8008	8-11
SECURITY FORMS	8009	8-12

Security Manager, delineating the results of the drill and any recommendations that would improve the present plan. A record of these drills will be maintained a minimum of two years.

7006. PRIORITY FOR EVACUATION/DESTRUCTION. The EAP will identify by type the priority for emergency evacuation and destruction of classified holdings. Priorities will be assigned per paragraph 17-8.2 of the reference.

7007. SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIF)
AND COMSEC FACILITIES

1. The SSO will prepare an EAP per the M1 manual and other applicable directives. A file copy will be made available to the Security Manager.
2. The CMS custodian will prepare an EAP for all COMSEC material per CSP1A, CMS4L, and other applicable directives. A copy will be provided to the Security Manager.
3. The SSO and CMS custodian will coordinate their respective EAP's with the OIC, CMCC.

cleared persons. All other Top Secret and Secret material will have destruction recorded on OPNAV Form 5511/12 (Classified Material Destruction) or on any other record which includes complete identification of the material, number of copies destroyed, and the date of destruction. Destruction records will be maintained for a minimum of two years. Confidential material not bucktagged by the CMCC may be destroyed without a record of destruction.

7003. EMERGENCY PLANS. In an emergency involving the danger of loss or compromise of classified material or equipment, the importance of beginning removal or destruction early cannot be overemphasized. All personnel shall be indoctrinated in emergency removal/destruction procedures. When required, the senior person present will initiate the necessary action without waiting for specific orders from higher authority. A periodic review (at least annually) of classified material holdings to identify material that is no longer needed is essential to reduce the amount of material that must be moved or destroyed.

1. Emergency Action Plans (EAP). Every command that stores classified material is required to develop an EAP for the protection of classified material in case of natural disaster, civil disturbance or enemy action. The EAP will provide for the protection of classified information in a way that will minimize the risk of injury to personnel.

2. CMCC EAP. The CMCC will maintain an inventory of all classified material evacuated, relocated or destroyed. SCP's will provide all requested information to the CMCC in an expeditious manner. The OIC, CMCC is responsible for developing an EAP that includes the CMCC and all SCP's/SCCP's in the MARRESFOR Headquarters and will coordinate the CMS and SCIF EAP to ensure all classified material is appropriately safeguarded. The MARRESFOR Security Manager will review and approve EAP's for the MARRESFOR Headquarters.

7004. EMERGENCY DESTRUCTION. All deployable commands must address the emergency destruction of classified information in their EAP. This requirement applies to all subordinate units except MCRSC. EAP's must be practical and reasonable additional information can be found in paragraph 17-7 of the reference.

7005. EMERGENCY ACTION DRILLS. All units holding material or equipment will conduct an emergency action drill at least annually. The purpose of this drill is to determine the effectiveness of the EAP and to familiarize personnel with emergency procedures. A written report will be made to the

SOP FOR ISP

CHAPTER 7

DESTRUCTION OF CLASSIFIED MATERIAL

7000. GENERAL. Chapter 17 of the reference sets forth those guidelines and procedures for the destruction of classified material and equipment within the Department of the Navy. Classified material will be destroyed as soon as it is no longer required by the unit/site. Material will not be retained for more than five years from the date of origin. All bucktagged classified material will be turned into the CMCC for destruction.

7001. METHODS OF DESTRUCTION. Classified material and equipment may be destroyed by those methods outlined in paragraph 17-3 of the reference. Any of these methods may be utilized so long as they preclude later recognition or reconstruction of the material or equipment.

1. MARRESFOR Headquarters. The CMCC, SPINTCOM, and G-2 is equipped with a shredder that meets the requirements for the destruction of classified material.

2. Subordinate Commands. Security managers and CMCC custodians will establish a means of destroying their classified holdings. The means and procedures of destruction will be identified in the unit SOP. When considering destruction equipment or means, paragraph 17-5 of the reference provides a listing of factors to consider in making a reasonable and economical decision.

7002. DESTRUCTION PROCEDURES

1. Classified material will be destroyed only by authorized means by personnel cleared to the level of the material being destroyed.

2. Classified material will be destroyed in the presence of two individuals and both individuals will have a security clearance commensurate with that of the material being destroyed. The two individuals conducting the destruction will sign the destruction report verifying the accuracy and complete destruction. The same two individuals cannot witness two consecutive reports.

3. Destruction of Top Secret and Secret material will be recorded. Exception to this is made for Secret/Confidential messages that are not controlled (bucktagged) by the CMCC. These messages may be destroyed by the SCPC without a record of destruction if destruction is performed or witnessed by two

SOP FOR ISP

CHAPTER 7

DESTRUCTION OF CLASSIFIED MATERIAL

	PARAGRAPH	PAGE
GENERAL	7000	7-3
METHODS OF DESTRUCTION	7001	7-3
DESTRUCTION PROCEDURES	7002	7-3
EMERGENCY PLANS	7003	7-4
EMERGENCY DESTRUCTION	7004	7-4
EMERGENCY ACTION DRILLS	7005	7-4
PRIORITY FOR EVACUATION/DESTRUCTION . .	7006	7-5
SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF) AND COMSEC FACILITIES	7007	7-5

SOP FOR ISP

HEADING

5510
(SECTION)
Date

From: (Section Head)
To: OIC, CMCC

Subj: COMPLETION OF SECONDARY CONTROL POINT (SCP)/SUB-CUSTODY
CONTROL POINT (SCCP) DIS-ESTABLISHMENT FOR THE (SECTION)

Ref: (a) (Section) MARRESFOR, ltr (list old letter data)

1. Per paragraph (7) of the reference, all actions indicated in the reference have been completed.
2. The SCP/SCCP located in (Section) has been disestablished.

Signature

Copy to:
SecMgr

SOP FOR ISP

HEADING

5510
(SECTION)
Date

From: Secondary Control Point Custodian (Section)
To: OIC, CMCC

Subj: NOTICE OF INSPECTION AND DEACTIVATION OF SECURITY CONTAINER

Ref: (a) ForO P5510.1

1. Per the reference the security container(s) listed below has/have been inspected by the undersigned, are devoid of classified material, the factory combination set, and are ready for turn-in/reissue. All container drawers were removed and a thorough search of the interior conducted.

CONTAINER SERIAL NUMBER

SCP/SCCP HAVING PRIOR CUSTODY

Signature

Copy to:
Supply Officer

SOP FOR ISP

7. When all actions listed above are completed, this section will notify the Security Manager and OIC CMCC.

Signature

Copy to:
SecMgr

SOP FOR ISP

HEADING

5510
(SECTION)
DATE

From: (Section Head)
To: OIC, CMCC

Subj: NOTIFICATION OF SECONDARY CONTROL POINT (SCP)/SUB-CUSTODY
CONTROL POINT (SCCP) DIS-ESTABLISHMENT FOR THE (SECTION)

Ref: (a) ForO P5510.1

Encl: (1) Inventory dated (date)

1. This section no longer has a requirement for a SCP/SCCP (If a SCCP, list specific area (Ops, MC&G, Trng, MMO, etc.)) and will be disestablishing that SCP/SCCP. Per the reference, the following applies:

a. Anticipated completion date:

b. Name of the SCPC/SCCPC:

2. Upon receipt of this letter, request that the OIC CMCC no longer route classified material to this SCP/SCCP.

3. As evidenced by enclosure (1), an inventory of all classified material has been conducted. Instructions are provided next to each line item detailing specific retention of materials and which SCP should gain custody, or the necessity for destruction of the material entirely.

4. As coordinated between this office and the CMCC, all classified materials will be returned to the CMCC on (list date).

5. Once all material has been transferred, this section will conduct an inspection of the control point area for classified material adrift, and ensure the area is free of classified material.

6. All security containers no longer required will be returned to HqBn Supply.

SOP FOR ISP

HEADING

5510
(SECTION)
DATE

From: (SCPC, Section)
To: OIC, CMCC

Subj: ACCESS AND AUTHORIZATION TO RECEIPT FOR CLASSIFIED MATERIAL
FOR (SECTION)

Ref: (a) ForO P5510.1

1. Per the reference the following individuals are authorized to
receipt for classified material for the (Section):

NAME	RANK	SSN	CLN	ACCESS
GISH, J. E.	SSGT	123456789	S	S/NS
DOOR, W. T.	LCPL	987654321	TS	TS/NS

Signature

Copy to:
Security Manager
Each Individual

SOP FOR ISP

HEADING

5510
ID
DATE

FIRST ENDORSEMENT on (Basic Request) ltr 5510 (ID) of (DATE)

From: OIC, CMCC

To: General or Special Staff Officer

Subj: AUTHORITY TO ESTABLISH A SECONDARY CONTROL
POINT/SUB-CUSTODY CONTROL POINT

Ref: (a) ForO P5510.1

1. Readdressed and returned, approved/denied (if denied provide justification).

2. Per the reference, and based on the Physical Security Evaluation certified in the basic correspondence, you are authorized to store classified material up to and including (Top Secret, Secret, or Confidential) in the containers listed in paragraph 4 of the basic correspondence. Open storage of (Top Secret, Secret, or Confidential) (is or is not) authorized.

3. This authority becomes invalid if any of the following occurs: there is a change in the General or Special Staff Officer; there is a change in primary custodian; there is a change in the security containers utilized, there is a change in physical location of the security container or if there is a change in the classification level of the material stored.

Signature

Copy to:
Security Manager

SOP FOR ISP

HEADING

5510
ID2
DATE

From: General or Special Staff Officer
To: OIC, CMCC

Subj: REQUEST FOR ESTABLISHMENT OF A SECONDARY CONTROL POINT
(SCP)/SUB-CUSTODY CONTROL POINT (SCCP)

Ref: (a) OPNAVINST 5510.1H
(b) ForO P5510.1

Encl: (1) Primary Custodian Appointment Letter
(2) Alternate Custodian Appointment Letter

1. Per Chapter 10 of reference (b), it is requested that (Staff Section) be authorized to establish an (SCP/SCCP) in (Office Number), (Building Number).

2. Justification:

3. Anticipated volume of material to be retained by security classification: (4 Drawer Secret, 2 Drawers Confidential)

4. Physical Security Evaluation: The proposed (SCP/SCCP) meets the physical security storage requirements of reference (a), Chapter 14 for the storage of (Top Secret, Secret, or Confidential) material/equipment in the following security containers:

<u>ROOM#</u>	<u>MANUFACTURER</u>	<u>SERIAL#</u>	<u>TYPE LOCK</u>	<u>SIZE</u>	<u>CLASS</u>
--------------	---------------------	----------------	------------------	-------------	--------------

5. (Grade, Name) has been designated the (SCP/SCCP) Custodian, enclosure (1), and (Grade, Name) has been designated as the Alternate (SCP/SCCP) Custodian, enclosure (2). I certify that the custodians have been fully briefed and are prepared to carry out their responsibilities per the references.

SIGNATURE

Copy to:
Security Manager

SOP FOR ISP

CMCC CHANGE FORM

Registered Mail # _____ Origin _____

Buck tag # _____ Copy # _____ Change _____

Date of Change _____

5310

From: Secondary Control Point
To: Officer in Charge, Classified Material Control Center

1. I do understand the attached change must be properly entered in the above listed buck tagged document within five (5) working days. All classified residue must be returned to the CMCC for destruction.

/S/

FIRST ENDORSEMENT

From: SCPO, _____
To: OIC, CMCC

1. I certify the above listed action was accomplished on _____ by _____, page checked by _____. All classified residue is attached herein.

/S/

SECOND ENDORSEMENT

From: OIC, CMCC
To: File

1. Classified residue destroyed and recorded on destruction report # _____ dtd _____.

/S/

Figure 6-6.--CMCC Change Form.

5-23

SOP FOR ISP

RECORD OF PAGECHECKS

[illegible]

Figure 6-4.--Page Check Form.

SOP FOR ISP

[illegible]

Figure 6-3.--Correspondance/Material Control (OPNAV 5216/10).

()

CLASSIFICATION	ORIGINATOR	SERIAL NUMBER	DATE OF DOCUMENT
SIFY ON		DOWNGRADE ON	
ED (DATE)/REPORT NUMBER		CURRENT CHANGES	
ERRED TO (COMPLAND)/DATE		REGISTERED MAIL NUMBER	
ICHE: YES NO QTY	DISKET YES NO QTY	DBASE/I	
YES NO QTY		DBASE/O	
YES NO QTY			
GRAPHS: YES NO QTY			
ARENCY: YES NO QTY			
		CHCC	

[illegible]

SOP FOR ISP

OPNAV 5511/10 (REV. 4-79)
S/N 0107-LF-055-1151

RECORD OF RECEIPT
(REFERENCE SECNAVINST 5216.5)

THIS RECEIPT MUST BE
SIGNED AND RETURNED.

ORIGINATOR'S CODE	FILE OR SERIAL NUMBER	DATE OF MATERIAL	UNCLASSIFIED DESCRIPTION	COPY NO.	NO. OF ENCLS. TO MATL RCD	REGISTERED NUMBER
<div style="position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%) rotate(-45deg); font-size: 100px; opacity: 0.5;"> SAMPLE </div>						

ADDRESSEE (ACTIVITY RECEIVING MATERIAL)

SIGNATURE (AUTHORIZED RECEIPT)

DATE

Figure 6-1.--Document Receipt.

9. CMS Custodian. The CMS Custodian is responsible for the accounting, control, handling, and administration of all COMSEC messages.

6018. FACSIMILE, EMAIL, AND OTHER ELECTRONICALLY RECEIVED DATA

1. All classified facsimile or EMAIL documents received directly by sections from outside the Headquarters must be routed to the CMCC for processing.
2. All classified data received via electronic transfer (computer files, programs, etc.) must be routed to the CMCC for accounting/control processing if that data is converted to a printed document. If data is captured or saved in an electronic file it must be transferred to the appropriately marked and controlled classified diskette and accounted for in accordance with procedures outlined in Chapter 12.
3. Documents used as "working papers" or research data, and retained for less than 90 days can be handled as Working Papers per the provisions of paragraph 6009.

made, however all entries will be made on the material receipt indicating disposition of the message.

d. Formal accountability, control, and destruction procedures and records will continue to be required for all other types of classified messages to include messages carrying such caveats as PERSONAL FOR, LIMDIS, NATO, and other special access or SPECAT categories.

5. Accountability

a. General Service U.S. Secret messages distributed within this Headquarters (including to the 4th MAW, 4th MarDiv, and 4th FSSG) will not be bucktagged (except those described in paragraph 6017.5b). These messages will be controlled by CMCC by recording the ORIGINATOR, DTG, SUBJECT, SCP routed to, and the date received before transferring them to the SCP. The SCPC will maintain a copy of receipts when the message is returned to the CMCC for transfer or destruction. If the message is subsequently transferred outside of this Headquarters then it must be sent to the CMCC for Bucktag number control.

b. NATO, LIMDIS, PERSONAL FOR, and other special access/special category Secret messages are accountable documents and will be issued a bucktag number. A log book/automated file containing the following columns will be used:

- Date Time Group
- Message Copy Number
- Originator
- Subject
- Special Access/Special Category Type
- Disposition

6. Top Secret. The TSCO will receipt for all Top Secret messages received by this Headquarters and will control the messages in the same manner described for a Top Secret Document. Signed receipts and destruction records are required for Top Secret messages. No Top Secret message will be left unattended or delivered to another section without first being delivered back to the TSCO.

7. Sensitive Compartmented Information (SCI). The Special Security Officer (SSO) is responsible for the accounting, control, handling, and administration of SCI messages.

8. SPECAT/Focal Point Message Traffic. The appropriate SPECAT/Focal Point Control Custodian is responsible for the accounting, control, handling, and administration of all SPECAT/Focal Point messages.

the appropriate person according to a list provided them by the CMCC. The Communications Center may also notify the CDO. The CDO is NOT authorized to view, sign, or pick up Top Secret or SPECAT messages unless his name is on the access list for that category of material.

e. The CDO should obtain the following information from the Communications Center if possible:

- (1) Precedence of message (Flash, Immediate, etc).
- (2) Is the command an ACTION or INFO addressee.
- (3) Classification of message.
- (4) Unclassified subject line.

With this info the CDO can contact the appropriate ACTION Officer.

2. Marking. Marking of classified messages is accomplished by the Communications Center.

3. Retention. The CMCC will retain classified messages that are not transferred to a SCP as follows:

a. Secret and Confidential messages are retained for 90 days from the date of receipt.

b. Top Secret messages are treated as Top Secret documents and are retained according to the instruction provided on the correspondence/material control (OPNAV 5216/10) by the section TSCO.

4. Control and Destruction. OPNAV Notice 5510 dtd 31 Dec 1991 rescinded DON policy requiring specific records of destruction for general service (GENSER) U.S. Secret messages. U.S. Secret message control procedures for the MARRESFOR and subordinate units are as follows:

a. A record copy of each U.S. Secret message must be maintained in the unit CMCC for ninety days, if the message is not transferred and retained by a SCP, then destroy if no longer required.

b. Each record copy must list staff sections to which the message was routed.

c. Staff sections holding U.S. Secret messages must destroy them when no longer required. Destruction must be witnessed by two individuals. No written record of the destruction need be

will then be forwarded from the OIC, CMCC to the SCPC verifying the inventory with records held by CMCC.

2. Procedure. The CMCC will provide inventory lists to all SCP's. The SCPC's will physically sight and match to the inventory the following data elements:

- a. Control Number.
- b. Copy number.
- c. Date of Document.
- d. Subject of Document.
- e. Sections holding U.S. Top Secret material will also conduct page checks and annotate the page check form attached to the material. Discrepancies will be reported to the CMCC in the following format:

Discrepancy: Bucktag 149456 shows copy 001/001. The Document reflects copy 001/002.

Discrepancy: Bucktag 234567 is missing page A-1.

Discrepancy: Bucktag 148678 is not held by the G-2 SCP.

6017. PROCESSING OF CLASSIFIED MESSAGES

1. Receipt. Classified messages are picked up from the Communications Center by personnel authorized in writing by the Commanding General, MARRESFOR (Unit Commander). Flash or Immediate ACTION classified messages that are received at the Communications Center after normal working hours are handled as follows:

- a. The Communications Center notifies the MARRESFOR CDO that a classified Flash or Immediate message has been received.
- b. The CDO is only authorized to VIEW Secret and below messages at the Communications Center window to determine what further action needs to be taken. The CDO will NOT take the message away from the Communications Center.
- c. If the message requires immediate attention the CDO will notify the appropriate section action officer and a CMCC clerk to respond to pick up the message from the Communications Center.
- d. If the message is classified Top Secret or is a Special Category (SPECAT) Message the Communications Center should notify

attached Correspondence/Material Control Form (OPNAV 5216/10), the recommended disposition of the document and return it to the SCP personnel for further delivery to the CMCC. Entries will be made in the SCCP log book indicating the disposition of the document, date returned, and signature of the SCP personnel.

c. SCCP Control Procedures. Appointed SCCP personnel will enter the material information into the SCCP Classified Document/Material Log book, which will contain at a minimum:

- (1) Bucktag number.
- (2) Copy number.
- (3) Date of document.
- (4) Subject (if classified, write "Classified Subject").
- (5) Disposition (Date returned to SCP for disposition include room in column for signature of SCP personnel).

6. SCCP Temporary Loan Within the SCP/Headquarters Building. Documents held by the SCCP may not be loaned temporarily overnight to other SCCP's within the SCP, or other SCP's within the Headquarters building. The same day temporary loan and return of bucktagged documents is authorized. A classified material control card will be utilized to identify the location of the material outside the SCCP.

7. Confidential Documents/Materials. Appointed SCCP personnel will receipt for the material from the SCPC. The procedures are the same as for the SCP.

6016. INVENTORIES

1. Frequency and Scope. SCP's will conduct inventories semi-annually, upon change of SCPC/SCCPC, or as directed of all bucktagged classified material held. The SCPC is responsible for the actual sighting of each and every document listed on the inventory supplied by the CMCC. In addition, the SCPC will also review each document for de-classification and any downgrading actions required and/or retention requirements. The SCPC will ensure that all SCCP's Log books reflect the correct information. The inventory provided by the CMCC will be endorsed back to the CMCC for final resolution listing those discrepancies that could not be resolved by the SCPC. The SCPC will certify each and every page of the inventory next to the CMCC inventory certification stamp. With assistance from the SCP concerned, the CMCC will review and resolve each discrepancy. A letter of verification

SCP receipt card file.

- d. Return of Materials to the CMCC. The Correspondence/ Material Control Form (OPNAV 5216/10) will be annotated and signed (block 5) to show desired action (retain indefinitely, retain XX months, or destroy after routing) for bucktagged materials returned to the CMCC. If material is to be transferred to another command, then instructions in the remarks section are appropriate.
- e. Confidential Documents/Materials. Confidential material retained by SCP's will be signed for from the CMCC. Unless otherwise required (see paragraph 6008 above) there will be no bucktag number on the document. Confidential material will be logged in a separate log (if a manual system is used) and the same information as for Secret material will be recorded except the bucktag number if none exists. This is done for control purposes. When this material is transferred to the CMCC a log entry will be made indicating the date and disposition. A separate file for copies of receipts of transferred Confidential should be maintained.

6015. SCCP ACCOUNTING AND CONTROL MEDIA

1. SCCP Classified Material Receipt Card. Prepared by the SCCP to indicate SCCP internal distribution. All applicable data is required to be transposed from the basic document and maintained current.
2. Correspondence/Material Control (OPNAV 5216/10). Described above in paragraph 6014.4b.
3. SCCP Bucktagged Material Log. A control measure maintained by the SCCP to identify the classified item and disposition. All applicable data is required to be entered from the basic document to the log book columns.
4. Inventories. Described in paragraph 6014.2d.
5. SCCP Procedures for Bucktagged Material
 - a. Receipt by SCCP Personnel. Appointed SCCP personnel will sign the SCP Classified Material Control Card for all bucktagged classified material that is delivered to the SCCP.
 - b. SCCP Personnel Review for Disposition. SCCP personnel will periodically review (at least semi-annually) each item for retention or other disposition after receipt. If retention of the material is not warranted, SCCP personnel will indicate on the

SOP FOR ISP

that is used to record NATO Secret-bucktagged material. Top Secret diskettes will be recorded in the log book that is used to record Top Secret bucktagged material.

d. Inventories. An accounting measure conducted semiannually (January and July), upon change of responsible individuals (SCPC, SCCPC), or as directed by the Security Manager, OIC, CMCC or other responsible individual.

3. SCP Accounting and Control Procedures for Secret Material

a. Receipt by the SCP Personnel. Only appointed SCP personnel will receipt for bucktagged classified material from the CMCC by signing the CMCC Classified Material Control Card, ensuring that the card information matches the information on the classified material.

b. SCP's Document Log. Separate logs will be maintained for the following categories of material: Bucktagged U.S. Top Secret material (includes Top Secret Diskettes), Bucktagged U.S. Secret material (includes Secret Diskettes and JCS Publications), NATO Secret material (includes NATO Secret Diskettes), and Special Access/Special Category messages (see paragraph 6017.5 of this Manual). Since no sections are authorized to retain NATO Top Secret Material overnight, no logs are required. The SCP incoming log shall contain at a minimum the following columns of information:

(1) Bucktag number.

(2) Copy number.

(3) Date of document.

(4) Subject.

(5) Disposition (date returned to CMCC for Destruction, Transfer, Retention, include room in column for signature of CMCC clerk if desired by SCPC).

c. Distribution to the SCCP. The following steps will be taken:

(1) SCP personnel will prepare a SCP classified material control card and make appropriate entries in the log book.

(2) Appointed SCCP personnel will receipt for the classified items, or indicate appropriate action to the SCPC, if not taking physical custody of the material.

(3) The SCP will retain custody of the receipt card in the

2. Conduct an inventory of all classified material in the custody of the dis-established control point. Provide the inventory to the CMCC, indicating the necessity for retention of specific materials, which SCP should gain custody, or destruction.
3. Return all classified material to the CMCC.
4. Inspect the dis-established control point area for classified material adrift.
5. Initiate action for the distribution or turn in of security containers held by the dis-established control point. Ensure figure 6-11 is completed and attached to each security container.
6. Report in writing to the OIC, CMCC of the completion of DIS-ESTABLISHMENT procedures, figure 6-12. A copy is sent to the Security Manager.

6014. SCP ACCOUNTING AND CONTROL PROCEDURES

1. The SCPC, ASCPC, and SCP Clerk are the SCP administrative personnel authorized to receipt for bucktagged classified material from the CMCC. Personnel appearing on the HQ MARRESFOR access roster may receipt for non-bucktagged classified material from the CMCC. Top Secret Material will be handled by designated Section TSCC/TSCA authorized in writing to the MARRESFOR TSCO.
2. SCP Accounting and Control Media
 - a. SCP Classified Material Control Card. This card is used to control and record the distribution of Secret and above documents and material within the SCP. A receipt card will be used in conjunction with Log books. All applicable data is required to be transposed from the basic document to the SCP Classified Material Control Card.
 - b. Correspondence/Material Control (OPNAV 5216/10). This form will be affixed to all bucktagged classified material by the CMCC prior to initial routing. Additional routing will be indicated by the SCPC on this Control Form. This form is also used to indicate to the CMCC the recommended disposition (Block 5) of classified documents returned to the CMCC from the SCP/SCCP.
 - c. SCP Document Logs. SCP central control measure for the receipt and distribution of material classified Secret and above which have been assigned a CMCC Bucktag Control Number. Separate logs will be maintained for different classifications/categories of bucktagged material. U.S. Secret diskettes will be recorded in the log book that is used to record U.S. Secret bucktagged material. NATO Secret diskettes will be recorded in the log book

materials are accurately entered into their account prior to routing the material within their section.

n. Ensure that classified "working papers" are not dormant and stored over 90 days. After that time, they must either be destroyed by the section or delivered to the CMCC for control.

o. Ensure that classified working papers are dated and marked with the highest classification contained therein when created.

p. Ensure that strict compliance with administrative and security requirements contained in the reference are maintained.

q. Ensure that all Top Secret material is accounted for by a continuous signed chain of receipts and returned to the TSCO when no longer needed prior to the end of normal working hours, (unless section is authorized to store U.S. Top Secret material). All individuals viewing Top Secret material will sign the Record of Disclosure Form.

r. Ensure that combinations to all security containers are changed per the time frames established in the reference and this Manual (no less than annually).

s. Ensure that the Security Container Information (SF 700) form packets with the actual combination inside (Not Part 1, which is to be attached to the inside of the container) are stamped with the highest classification of material they protect.

t. Ensure that Turnover Files/Desktop Procedures are prepared and maintained per paragraph 2002 of this Manual to facilitate the "in briefing" of personnel assuming custodial duties.

u. Periodically review the classified holdings and identify material that is no longer needed and can be returned to CMCC for destruction.

6013. SCP/SCCP DIS-ESTABLISHMENT PROCEDURES. When the requirement for a SCP/SCCP no longer exist, the following procedures will be completed by the General or Special Staff Section Head, the Commanding Officer, HqBn, MARRESFOR or the unit Security Manager:

1. Use figure 6-10 to notify in writing the OIC, CMCC of the intent of DIS-ESTABLISHMENT, indicating the anticipated completion date, and the name of the SCPC. Classified material will no longer be routed to that control point upon receipt of the letter by the CMCC.

6010. SECONDARY CONTROL POINTS/SUBCUSTODY CONTROL POINTS

1. SCP's are subordinate satellite classified material storage control areas of the CMCC. They are established when the CMCC cannot adequately support the daily requirement for classified material at the section level. SCP's are subordinate to the CMCC. Each section may establish only one SCP. Large sections may establish Sub Custody Control Points if necessary.
2. SCCP's are subordinate satellite classified material storage and control areas of SCP's. They are established when the SCP cannot adequately support the daily requirements for classified material at the sub-section level. For example, a staff section with an office in another building which continuously (daily) makes trips to the SCP for necessary classified material could consider establishing a SCCP. SCCP's are subordinate to their parent SCP.
3. SCP's are responsible for ensuring the timely return to the CMCC of all controlled classified documents not actually in use or those documents designated for destruction.
4. SCP's/SCCP's may not retain classified material above the level specified in their establishment authorization. No SCP/SCCP is authorized to store COSMIC Top Secret material overnight.

6011. DESIGNATION OF SCP'S/SCCP'S

1. Requests for Establishment. General and Special Staff Section Heads will request in writing from the MARRESFOR/subordinate unit OIC, CMCC (utilizing figure 6-7 request to establish an SCP/SCCP). The request will include:
 - a. A justification statement;
 - b. The location (office number and building) of the control point;
 - c. A list/description of the security containers, with serial numbers;
 - d. The designation of a Control Point Custodian and alternate (refer to chapter 2 of this Manual for letter format and rank requirements);
 - e. A description of the anticipated volume of material to be retained by security classification;
 - f. Certification that the custodians have been fully briefed

f. Establish and maintain records for all controlled classified material checked out to their SCP and any SCCP under their control.

(1) Green standard Log books will be used, and may be supplemented with automated systems for controlled material accountability. SCPC's will also keep a record of the location of all documents held within the SCP. These logs will become a permanent part of the SCP files and will be retained for a period of two years after the log book had been officially closed.

(2) SCCP's may retain NATO documents and messages only if authorized by their current PSE. All SCP/SCCP personnel must have the appropriate NATO clearance and access prior to handling NATO classified material. All SCPC's/SCCPC's will ensure that all NATO classified material is filed separately from all other classified material, and is easily identifiable if stored in the same drawer as U.S. classified material.

g. The SCPC may designate personnel to receipt for classified material using figure 6-9 "Access and Authorization to Receipt for Classified Material". This Authorization record will be held in the CMCC. Once receipted for, this material becomes the responsibility of the SCPC.

h. Hold current Security Container Information (SF 700) envelopes (less COMSEC) with combinations to all SCP/SCCP security containers in a designated "master safe". Combinations to COMSEC containers will be wrapped per appropriate communications security regulations and will be delivered for storage to the CMCC for emergency action contingencies. SF 700 is the only form authorized to record security container combinations. The top cover sheet of a SF 700 will be attached to the outside of the container to which it corresponds.

i. List the priority of removal/destruction of classified material as outlined in the section's Emergency Action Plan.

j. Ensure that SCP/SCCP personnel do not destroy controlled Secret and above documents (including Confidential diskettes). These documents will be returned to the CMCC for destruction.

k. Ensure the SCP/SCCP files are maintained in an orderly manner to avoid loss and/or accounting errors.

l. Ensure that SCP/SCCP personnel are thoroughly instructed on the nature and importance of their duties.

m. Ensure that SCP Clerk's/SCCP Clerk's examine all controlled materials for completeness upon receipt and ensure the

SOP FOR ISP

and are prepared to carry out their responsibilities per this Manual and the reference.

2. A new request must be submitted if any of the following occurs:

- a. There is a change in the General or Special Staff Officer;
- b. There is a change in primary custodian;
- c. There is a change in the classification level of the classified material stored;
- d. There is a change in location of the security containers.

3. The MARRESFOR OIC, CMCC/subordinate unit OIC, CMCC will review the request for establishment of SCP/SCCP and provide written approval/disapproval (utilizing figure 6-8). If approved, the letter will list the volume and highest classification of material authorized for custody by the control point. A copy of the letter will be provided to the Security Manager and will be retained permanently in the SCP/SCCP Turnover/Desktop procedures.

6012. DETAILED SCPC/SCCPC RESPONSIBILITIES

1. SCPC's/SCCPC's are responsible for the control and protection of all classified material brought into their respective section.

2. The SCPC/SCCPC will:

- a. Periodically review the level of security clearance and access of each person assigned to the section and, when required, initiate action through the Section Head, to upgrade or downgrade individual clearance and access. Such requests will be forwarded to the MARRESFOR HqBn Security Manager or the Unit Commander.
- b. Ensure that only authorized personnel have access to classified material.
- c. Ensure the section receipt authorization record is current and take corrective action when not.
- d. Maintain and provide to the CMCC a listing which shows current clearance and access of all individuals in their sections.
- e. Expeditionously route classified materials to cognizant personnel within their section and promptly return all controlled materials to the CMCC for additional routing, transfer, or destruction as required.

will be taken to the CMCC for destruction. The CMCC will give the SCP a receipt for the document(s) and then destroy it. No record of destruction is required for Confidential material, however the log will be annotated to reflect the disposition of the document(s).

6009. WORKING PAPERS

1. Working papers are documents and material accumulated or created while preparing finished material (i.e., rough drafts). As a minimum working papers containing classified information shall be:

- a. Dated when created;
- b. Marked on each page with the highest classification of any information contained therein;
- c. Protected per the classification assigned;
- d. Destroyed when no longer needed; and
- e. Accounted for, controlled, and marked in the manner prescribed for a finished document of the same classification when:

(1) Released by the originator outside the command or transmitted electrically or through message center channels within the command;

(2) Retained more than 90 days from the date of origin (If classified notes and messages relating to one subject area or project are maintained in one binder or folder, the entire package of material can be considered a working paper and will be dated when created. However, if materials are added to or removed from a dynamic package (e.g. long term project/exercise) during that 90 day period, the whole package may be re dated thus restarting the 90 day clock. When the project/exercise has ended and the package is dormant, it then must be controlled 90 days from the last date placed on the package);

(3) Top Secret information is contained therein; or

(4) Filed permanently.

2. Classified notes from a training course or conference are considered working papers.

2. Secret/NATO. All changes to U.S. Secret documents will be accomplished by the section that holds the basic document. The following procedures will be followed: .

a. The CMCC will receive the change and label the change with the bucktag number of the original document. The subject will be prefixed with the appropriate change number (ie., 612345 CHANGE 1). Figure 6-6 will be attached to the document, and the document will be added to the CMCC log book/data base.

b. The section will sign for the change on the back of the original document control card and will have five working days to enter the change and return the change residue (residue is the pages that have been replaced and removed) to the CMCC for destruction. NO SECTION IS AUTHORIZED TO DESTROY SECRET CHANGE RESIDUE. SCPC's are reminded to pay special attention to the list of effective pages that accompanies documents to ensure that only like for like pages have been removed and returned to the CMCC. The time to discover original pages missing, is before the residue has been destroyed.

c. The CMCC will maintain a copy of the change residue route sheet in a tickler file and will monitor same. Once change residue has been returned back to the CMCC, the appropriate destruction report will be prepared and the residue appropriately destroyed.

3. Confidential/NATO. All changes to confidential material will routed to the appropriate section for action.

6007. CMCC CLASSIFIED MATERIAL CONTROL CARDS. Classified Material Control Cards (Figure 6-2) will be signed each time documents change hands and will be retained in the CMCC in two categories, an on hand file and a checked out file, in order to track the documents' location within this Headquarters. SCP's/SCCP's will establish control by use of the same control cards. Signing of Log books is only authorized when the transaction indicates the final disposition (SCCP delivers material to SCP or SCP delivers material to the CMCC for transfer, destruction or routing to another SCP).

6008. PROCESSING AND HANDLING OF INCOMING CONFIDENTIAL MATERIAL. The CMCC will not assign control numbers to Confidential material. unless required by Caveat such as Personal For, LIMDIS, or NATO. CMCC will enter all Confidential documents received into a log. If the document is subsequently issued to a SCP for retention the SCP representative will sign the log entry receipting for the document. When the document is no longer needed by the SCP it

assemble the following forms: Classified Material Control Card (Figure 6-2), and Correspondence/Material Control (OPNAV 5216/10) (Figure 6-3). The next available control number will be assigned to the document, and the appropriate entries in the Secret Material Control Log book will be made. The following information will be stamped or affixed to the front cover of the document:

(unit)# _____ CONTROL NUMBER _____
REC'D _____ DATE _____
COPY _____ OF COPIES _____

The Correspondence/Material Control Form (OPNAV 5216/10) will be affixed to the front cover of the document, and the document control card will be paper clipped to the document. The record of receipt and the entire package will then be entered into the document control data base or log book. Upon completion, the document and control card will be placed in the appropriate section's box for further routing. The CMCC will only hold a single "official file copy" of classified documents. All other copies will be distributed as required or disposed of as indicated by the cognizant SCP. When only one copy of a document is received, the cognizant SCP will hold the official file copy. The CMCC document control card signed by the SCPC/SCPA will be the locating device for distributed documents. The SCPC/SCPA are the SCP administrative medium and are held accountable for the material until delivered to the SCCPC/SCCPA or returned back to the CMCC.

6005. ROUTING. Initial routing of Secret and Top Secret material will be indicated on the Correspondence/Material Control Form (OPNAV 5216/10) by the CMCC. Sections will be contacted via EMAIL or telephone, alerting that classified material is held in the CMCC for them. The primary action section will ensure that all cognizant staff sections are included in the routing instructions and that the retention instructions have been noted on the control form. Further routing of Top Secret material to other than the primary action section will be on a strict need-to-know basis. Retention periods are computed from the date the document is received by this Command. Thus, a document received on 10 March 1990, and marked "Retain 6 months" would be destroyed on 9 September 1990 by the CMCC without further instructions.

6006. PROCESSING AND HANDLING OF CHANGES TO U.S. AND NATO CLASSIFIED MATERIAL

1. Top Secret/NATO. All changes to Top Secret, COSMIC/ATOMAL, or NATO Secret documents will be handled specifically by the TSCO or the NATO Sub-Registry COSMIC/ATOMAL Control Custodian.

(2) ATOMAL. The same numbering procedures apply for ATOMAL except the first digit is a three (3) vice (2). A sample number is 393005.

b. Copy numbers assigned to NATO Top Secret documents will be the same as the originator's copy number.

c. The NATO Sub-Registry COSMIC/ATOMAL Control Custodian will page check the document and annotate the page check form.

d. The identifying document information will be entered into the COSMIC/ATOMAL Top Secret automated data base and the document then held for pickup by the appropriate section.

e. No section is permitted to retain COSMIC/ATOMAL Top Secret material overnight. The material will be returned to the NATO Sub-Registry COSMIC/ATOMAL Control Custodian prior to the close of working hours.

6004. CMCC INCOMING SECRET MATERIAL. Incoming Secret documents will be controlled in the CMCC under the supervision of the OIC, CMCC. A document control number will be assigned to the material. The following control number sequences will be used:

1. U.S. Secret Documents. Assigned control numbers are the same as for U.S. and NATO Top Secret except the first number must start with a six (6). For example, 693007 is the seventh U.S. Secret document received in 1993.

2. JCS Secret Documents. Control numbers are assigned the same as for U.S. Secret documents.

3. CNWDI. Control numbers are assigned as described above for Top Secret, except that the first digit is (4). For example, 493003 denotes the third CNWDI document received in 1993.

4. NATO Secret Documents. Control numbers are assigned as described above for U.S. Secret, except that the first digit is a five (5). For example, 593005 is the fifth NATO Secret document received in 1993.

5. Processing and Handling of Incoming Secret Material. Upon receipt, CMCC personnel will inspect the package for signs of tampering. If none is detected, the package will be opened. If signs of tampering exist, the OIC, CMCC and Counterintelligence Representative (if assigned), or Security Manager will be notified. When the package is opened, the material will be verified against the data appearing on the return receipt. CMCC personnel will sign and return the receipt. CMCC personnel will

b. Handling of Top Secret Material. Routing of the document will be accomplished by use of the Correspondence/Material Control Form and the Top Secret Disclosure Sheet. Only designated sections may retain U.S. Top Secret material overnight. Only the section appointed TSCC or TSCA (must be designated in writing by the TSCO) may receipt for Top Secret material on route or on temporary loan from the TSCO. The TSCO or TSCA must page check the document for completeness prior to leaving the CMCC. In addition, all persons physically handling the material must have authorized access to Top Secret material and must sign the Top Secret Disclosure Sheet.

c. No intra or inter-section routing of Top Secret material is permitted. Once action is completed in one section, the document must be returned to the TSCO for routing to the next section. For example, a document annotated for routing to the G-2 and G-3 may initially be routed to the G-2 but must be returned to the TSCO for routing to the G-3. If the document is viewed by anyone other than the Section Head the name of the person must be annotated on the record of disclosure.

d. During each intermediate stop at the CMCC, the TSCO will review the document disclosure sheet to ensure that only persons authorized access to Top Secret material have handled the document, and a page check will be conducted prior to acceptance by the TSCO.

e. The authorized section TSCC/TSCA is responsible for the proper handling and integrity of the material in that persons care. Minimal amounts of Top Secret material will be held within this Headquarters. In most cases, a single copy of each Top Secret document will suffice. Primary action sections are responsible for indicating the retention period of the document on the Correspondence/Material Control Form.

2. Control procedures for NATO classified material mirrors those used for U.S. classified material except that the NATO Sub-registry Control Point/COSMIC/ATOMAL Control Custodian and assistant will process all NATO documents within the CMCC and NATO Confidential must be sent by Registered mail. NATO Top Secret is designated either COSMIC or ATOMAL.

a. The control numbers assigned to NATO Top Secret documents are as follows:

(1) COSMIC. A sample number is 293005. The first digit indicates that the document is COSMIC. The second and third digits (93) indicate the calendar year that the document was received (1993). The fourth, fifth, and sixth digits indicate the number of the document for any calendar year (the fifth COSMIC document received for 1993).

classified material. If no classified material is found then it will be returned to the mail room for delivery. The CMCC will return classified material receipts to originators.

6003. CMCC INCOMING TOP SECRET MATERIAL

1. Incoming Top Secret material will be controlled in the CMCC by the TSCO. The TSCO will assign a control number to the material. The following control numbering system will be utilized. The first digit is a one. The second and third digits reflect the calendar year in which the document was received. The fourth, fifth and sixth digits indicate the number of the document for any calendar year. For example, 193001 is the first U.S. Top Secret document received in 1993.

a. Processing of Incoming Top Secret Material. Upon receipt of a Top Secret document, the TSCO or assistant will inspect the package for signs of tampering. If none is detected, the package will be opened. If signs of tampering exist, the OIC, CMCC and the MARRESFOR Counterintelligence Representative will be notified. When the package is opened, the documents will be separated and verified to match the data appearing on the receipt. The TSCO or TSCA will sign the document receipt. The TSCO or TSCA will retrieve the appropriate Control Log and then assemble and put together the following forms: Classified Material Control Card (Figure 6-2), Correspondence/Material Control (OPNAV 5216/10) (Figure 6-3), Page Check Form (Figure 6-4), and the Record of Disclosure (Figure 6-5). The next available control number will be assigned to the document and the appropriate entries in the log book will be accomplished. The control card will be completed as well as the forms listed above, less the Record of Page Check Form. The following information will be stamped or affixed to the front cover of the document:

CG MARRESFOR # CONTROL NUMBER
REC'D DATE
COPY OF COPIES

The only copy number assigned to Top Secret documents received from other commands will be the copy number assigned by the originator. Both the TSCO and TSCA will page check the Top Secret document for completeness and accuracy and so annotate the Page Check Form. When these actions are complete the forms will be stapled on the document front cover in the following order (Top to Bottom): Correspondence/ Material Control (OPNAV 5216/10), Record of Disclosure, and the Page Check Form. The data will be entered into the Top Secret Document log book or automated data base and prepared for delivery to the appropriate section.

SOP FOR ISP

	FIGURE	PAGE
6-1	DOCUMENT RECEIPT	6-23
6-2	CLASSIFIED MATERIAL CONTROL CARD	6-24
6-3	CORRESPONDENCE/MATERIAL CONTROL (OPNAV 5216/10)	6-25
6-4	PAGE CHECK FORM	6-26
6-5	RECORD OF DISCLOSURE (U.S. TOP SECRET)	6-27
6-6	CMCC CHANGE FORM	6-28
6-7	FORMAT FOR REQUEST TO ESTABLISH SCP/SCCP	6-29
6-8	FORMAT FOR AUTHORITY TO ESTABLISH A SCP/SCCP	6-30
6-9	FORMAT FOR ACCESS AND AUTHORIZATION TO RECEIPT FOR CLASSIFIED MATERIAL	6-31
6-10	FORMAT FOR SCP/SCCP DIS-ESTABLISHMENT PROCEDURE	6-32
6-11	FORMAT OF NOTICE OF DEACTIVATION OF SECURITY CONTAINER	6-34
6-12	FORMAT FOR COMPLETION OF SCP/SCCP DIS-ESTABLISHMENT	6-35

SOP FOR ISP

CHAPTER 6

ACCOUNTING AND CONTROL

	PARAGRAPH	PAGE
CUSTODY AND ACCOUNTABILITY	6000	6-3
CMCC CONTROL RECORDS AND LOGS	6001	6-3
CMCC ACCOUNTING AND CONTROL PROCEDURES . . .	6002	6-4
CMCC INCOMING TOP SECRET MATERIAL	6003	6-4
CMCC INCOMING SECRET MATERIAL	6004	6-7
ROUTING	6005	6-8
PROCESSING AND HANDLING OF CHANGES TO U.S. AND NATO CLASSIFIED MATERIAL	6006	6-8
CMCC CLASSIFIED MATERIAL CONTROL CARDS . . .	6007	6-9
PROCESSING AND HANDLING OF INCOMING CONFIDENTIAL MATERIAL	6008	6-9
WORKING PAPERS	6009	6-9
SECONDARY CONTROL POINTS/SUBCUSTODY CONTROL POINTS	6010	6-11
DESIGNATION OF SCP'S/SCCP'S	6011	6-11
DETAILED SCPC/SCCP RESPONSIBILITIES	6012	6-12
SCP/SCCP DIS-ESTABLISHMENT PROCEDURES . . .	6013	6-14
SCP ACCOUNTING AND CONTROL PROCEDURES . . .	6014	6-15
SCCP ACCOUNTING AND CONTROL MEDIA	6015	6-17
INVENTORIES	6016	6-19
PROCESSING OF CLASSIFIED MESSAGES	6017	6-19
FACSIMILE, EMAIL, AND OTHER ELECTRONICALLY RECEIVED DATA	6018	6-22

caveats on the document require a bucktag number (such as LIMDIS, PERSONAL FOR, ORCON). Each log shall contain at a minimum the following information:

- Bucktag number
- Registered Mail Number IN (DCS # IN for Top Secret logs)
- Date Received
- Registered Number OUT (DCS number OUT for Top Secret logs)
- Date Out
- Date of Document
- Originator
- Copy number
- Subject (if classified, write "Classified Subject")
- Remarks (date destroyed, transferred, etc.)
- Section SCP holding material

4. Log books will be retained for two years after being officially closed. Log books may not be closed until all documents recorded therein have had a final disposition. This does not preclude transferring document information to a new log book when necessary.

6002. CMCC ACCOUNTING AND CONTROL PROCEDURES

1. The CMCC is the initial control point for the receipt of all classified material with the following exceptions:

a. SCI material under the cognizance of the Special Security Officer (SSO).

b. SPECAT material under the cognizance of FOCAL Point Control Officer.

c. COMSEC material under the cognizance of the CMS Custodian.

2. Except for the above material, all personnel within MARRESFOR Headquarters will ensure that ALL classified material received directly by their section is delivered promptly and directly to the CMCC for entry into the Classified Material Control System.

3. The CMCC will process all classified material to include entry into the classified material control accounting system, package (less labels which sections will address), prepare receipts, and transmit (mail or fax) the material.

4. The mail room will not open registered or certified mail but will deliver all such mail (including any other mail that they believe may contain classified material) to the CMCC. The CMCC will open this mail and handle appropriately if it contains

SOP FOR ISP

CHAPTER 6

ACCOUNTING AND CONTROL

6000. CUSTODY AND ACCOUNTABILITY

1. The MARRESFOR Classified Material Control Center (CMCC) will receive, route, and account for all classified material addressed to Headquarters MARRESFOR, 4th MarDiv, 4th MAW, and 4th FSSG (except that material listed in paragraph 6002). Subordinate units not collocated with MARRESFOR; 2d MEB, 3d MEB, MCRSC (Unit Commanders) that hold classified material will establish a CMCC that will receive, route, and account for all classified material addressed to that command and any unit that it services.

2. CMCC control procedures for classified material begin with the receipt of any classified material. An accounting system as set forth in paragraph 6002 of this Manual will be maintained at the CMCC.

6001. CMCC CONTROL RECORDS AND LOGS. CMCC control records and logs will be manual, automated, or a combination of both, as long as the requirements published in this Manual are met. The CMCC shall maintain the following logs:

1. CMCC Outgoing Registered Mail Log. The CMCC outgoing registered mail log or automated file shall contain at a minimum the following information:

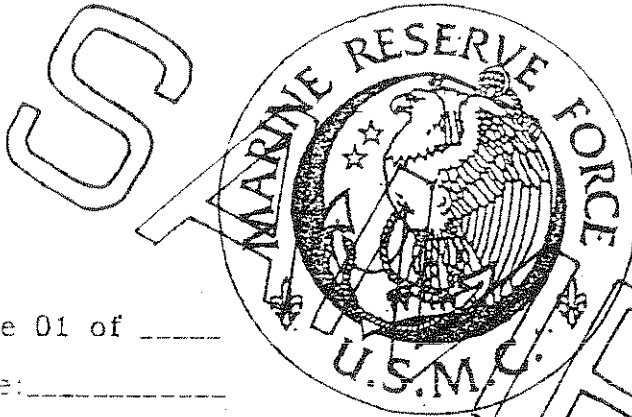
- Registered Mail Number
- Bucktag Number
- Copy Number
- Subject (if classified, write "Classified Subject")
- Originator
- Date Mailed
- Unit Document Mailed to
- Date Unit Received Document (based on return receipt date)
- Date HQ MARRESFOR (unit) received receipt
- Date Postal Tracer Sent
- Date Message Tracer Sent

2. Bucktag Control Number Log: The CMCC shall maintain separate logs for the following categories of controlled classified material: U.S. Secret, NATO Secret, and U.S. Top Secret.

3. Confidential Document Log. This log will be used to record the receipt of all Confidential documents. It will contain the same information as above except for bucktag number unless the

SOP FOR ISP

Classification: _____



Page 01 of _____

Date: _____

FROM

Name: _____

Section: _____

Voice Phone No.: _____

FAX No.: _____

TO

Name: _____

Section: _____

Voice Phone No.: _____

FAX No.: _____

Releasing Signature: _____

FOR CMCC USE ONLY

SUBJECT: _____

DATE TRANSMITTED: _____

TIME TRANSMITTED: _____

OPERATOR: _____

ACKNOWLEDGE RECEIPT BY: _____

(RANK/NAME/UNIT/SECTION)

BUCK TAG NUMBER
(IF APPLICABLE)

Figure 5-2.--Secure Facsimile Transmission Sheet.

SOP FOR ISP

d. You will have in your possession your armed forces identification card and the original of this letter. A sufficient number of certified true copies of this letter will be carried with you to provide copies to airline officials if requested.

e. You will arrange for appropriate storage of the classified material at your destination and upon your return to this station.

f. If you encounter any difficulty with airline security or other officials you are instructed to contact the Security Manager or the OIC, CMCC for assistance. If you are not allowed to board the aircraft without surrendering or opening the classified material you will terminate the travel and return the material to this Command.

4. By memorandum endorsement hereon you have certified that you have been fully briefed and understand your duties and responsibilities as outlined in Chapter 16 of the reference.

5. This authorization expires on (maximum time is one year).

J. J. DOE
By direction

Copy to:
CMCC
File

MEMORANDUM ENDORSEMENT

From: Gunnery Sergeant Dan Daley 123 45 6789/0311 USMC
To: Commanding General, Marine Reserve Force

Subj: AUTHORIZATION TO HAND CARRY/ESCORT CLASSIFIED MATERIAL

1. I certify that I have been briefed and fully understand my duties and responsibilities regarding the HAND CARRYING (escorting) of classified material.

2. I have inventoried with the CMCC and signed for all classified material in my possession. I have a copy of the inventory list in my possession and will return the classified material to the CMCC upon my return.

Signature

date

Figure 5-1.--Format for Authorization to HANDCARRY Classified Information--Continued.

SOP FOR ISP

HEADING

5511
SecMgr
(date)

From: Security Manager, Marine Reserve Force (unit)
To: Gunnery Sergeant Dan Daley 123 45 6789/0311 USMC

Subj: AUTHORIZATION TO HAND CARRY/ESCORT CLASSIFIED MATERIAL

Ref: (a) OPNAVINST 5510.1H
(b) ForO P5510.1

1. You have been authorized to hand carry classified material while in an official travel status within and between the United States, its Territories and Canada per the references. This authorization does/does not include travel on commercial passenger aircraft.

2. Your security clearance status is verified as Top Secret based on an SSBI conducted by the Defense Investigative Service on 1 Jan 1993. Your case control number is 93-00001. You have been authorized access up to and including Top Secret.

3. The following instructions for hand carrying/escorting classified material apply:

a. The material shall be enclosed in two opaque sealed envelopes of similar wrappings. The wrappings shall conceal all classified characteristics of the material. The inner envelope will be stamped with the classification of the enclosed material. The outer envelope will bear no classification or any other markings that would indicate its contents but will be addressed to this Command. The envelopes will be carried inside a locked briefcase.

b. The material will remain in your physical possession at all times during travel.

c. You will not permit the opening of the envelopes or reading of the material by airport security or any other official.

Figure 5-1.--Format for Authorization to HANDCARRY Classified Information.

b. The CMCC will request retransmission of all illegible or incomplete material.

c. Incoming material will be reviewed by the CMCC to ensure that it is properly marked and accountability is established per this Manual.

d. Sections will receipt for their material at the CMCC.

5006. TELEPHONIC TRANSMISSIONS. Classified information will not be transmitted over the telephone except as may be authorized on approved secure communication circuits.

1. Approved secure communication systems require equipment and operating procedures to place and receive calls that are quite different from those used for general telephone service. Unless the special equipment is being used, there is no reason to believe a line could be secure. In all other circumstances, the telephone system is not secure and any discussion of classified information or "talking around" classified information is prohibited.

2. A properly keyed STU-III telephone is the only authorized means to discuss classified information by telephone. Care should be taken to ensure that the classified conversation cannot be overheard by non authorized personnel in the vicinity of the telephone.

3. Transmission of classified data between computer systems must be accomplished only on accredited secure data circuits or via properly keyed STU-III telephones. Once transmission of classified information is complete the modem/STU-III must be physically disconnected from the computer if the classified data will be stored on the computer hard drive or if the computer is used to process classified data.

identification on the messages of where derivative classification was obtained.

5005. FACSIMILE AND OTHER ELECTRONIC DATA

1. The CMCC has the capability to transmit classified documents, via secure facsimile, to other facilities that also have a secure facsimile capability. To ensure adequate accountability and security for documents processed via this system, the following procedures apply:

a. The following types of classified material are not authorized for transmission via secure facsimile:

- (1) Material classified Top Secret.
- (2) Special Access Program Material.
- (3) Material marked with the caveat "ORCON".

b. The following procedures will be used when transmitting classified material via secure facsimile.

(1) All classified material requiring transmission will be forwarded to the CMCC. The top portion of a Secure Facsimile Transmission Sheet, Figure 5-2, will be completed by the SCPC.

(2) An authorized message releasing authority will sign the sheet in the space provided.

(3) The CMCC will ensure that the material to be transmitted is properly marked and authorized for transmission. Once this has been accomplished, the CMCC will complete the bottom portion of the Secure Facsimile Transmission Sheet.

(4) The CMCC will maintain a log of all classified material transmitted to or from via secure facsimile. At minimum, the log will contain the following information: Date/Time of transmission, BT# or Serial number, Classification, Subject (if unclassified, otherwise "Classified"), Command/section of origination, Command/section of destination.

2. For incoming material, the CMCC will complete the top portion of a Secure Facsimile Transmission Sheet and attach it to the material routed to the destination section SCP.

a. Illegible or incomplete incoming classified material will be treated as waste and will be destroyed by the CMCC.

(3) Authorization to HAND CARRY classified material is indicated in his/her original orders.

(4) The material is in double sealed envelopes and safeguarded from unauthorized personnel. (A briefcase or courier pouch may not be considered as the outer container in this circumstance.)

(5) Arrangements for the proper storage of the material at the individual's destination have been made. Classified material will not be maintained in hotel rooms or trunks of vehicles.

5. Transporting Classified Equipment. Classified equipment will be transported in the following manner:

a. If the classified equipment is an inaccessible component of a bulky item of equipment, then the equipment may be transported from one point to another without additional wrapping.

b. If the classified equipment is an item of equipment and the shell of the body is classified, then it shall be draped with an opaque covering that will conceal all classified features. The custodian or security manager of the storage area from which the equipment was drawn will ensure that this covering is capable of being secured so as to avoid/prevent inadvertent exposure of the item.

5004. NAVAL MESSAGES. The drafter of an outgoing classified message will be responsible for ensuring that all classification, de-classification, and review data is per the guidelines provided in the reference and other pertinent regulations.

1. MARRESFOR Communications-Electronic Officer (CEO). Within the MARRESFOR Headquarters, the CEO is responsible for reviewing all classified messages for format and delivering them to the communications center. SPECAT and other special access program messages will be routed through the CEO in such a manner that precludes the viewing of the body of the message. This paragraph does not apply to SCI messages handled through the MARRESFOR SPINTCOM.

2. Classified Message Releasing Authority. Within the MARRESFOR Headquarters classified messages will only be released by those personnel occupying the billets for classified message releasing authority identified in ForO P5000.1.

3. CMCC. The CMCC of all commands will be responsible for retaining a copy of all outgoing classified messages with

disclosure of that information or material. All provision of chapter 16 the reference will be adhered to where applicable.

1. HAND CARRYING Classified Material Inside a Building.

Personnel HAND CARRYING classified material inside a building, i.e., from one office space to another, will use an appropriate cover sheet e.g., (SF 704 Secret Cover Sheet) to reduce the possibility of unauthorized viewing.

2. HAND CARRYING Classified Material from one Building to Another.

Individuals HAND CARRYING classified material from one building to another will ensure the material is wrapped and use a briefcase or courier pouch to prevent the possibility of accidental loss or unauthorized viewing. The briefcase or courier pouch will be locked or sealed and bear no external marking to indicate that classified material is enclosed.

3. HAND CARRYING Classified Material While In A Travel Status.

The HAND CARRYING of classified material while in a travel status will be authorized only in those cases where the material is required at the traveler's destination and is not available there; or because of time or other constraints the classified material cannot be transported by other authorized means.

4. Authorization. The MARRESFOR, 4th MarDiv, 4th MAW, 2ndMEB, 3rdMEB, 4th FSSG, MCRSC, and HQBN Security Managers are the only individuals who can authorize personnel to HAND CARRY classified material while in a travel status inside the United States. Outside the United States and its territories, written authorization from the Commandant of the Marine Corps (ARAD) (via the chain of command) must be obtained prior to travel.

a. All authorizations to hand carry classified material must be in writing and signed by the appropriate Security Manager using the format depicted in Figure 5-1.

b. Personnel receiving authorization to HAND CARRY classified material will be briefed by the Security Manager on the provisions of chapter 16 of the reference and sign a statement acknowledging he/she received and understood the briefing. This statement will be retained by the Security Manager for two years. In addition the OIC, CMCC shall ensure:

(1) The CMCC prepares and maintains a written inventory of all classified material to be hand carried prior to the individual's departure and conducts another inventory upon the traveler's return.

(2) The individual has signed for the material from the CMCC.

Government civilian employees (see paragraph 5003, HAND CARRYING Classified Material and Equipment).

c. Secure telephonic transmission.

3. COMSEC material will be shipped/mailed per CMS 4-L (Communications Security Material System) and CSP-1 (Cryptographic Security Policy and Procedures).

4. SCI material is under the cognizance of the MARRESFOR SSO and will be shipped per the M-1 manual and other appropriate directives.

5002. RETURN RECEIPT SYSTEM. All classified material and equipment mailed or shipped from MARRESFOR Headquarters or subordinate units will have a return receipt card, OPNAV Form 5511/10, attached. The OIC, CMCC will establish a return receipt system to assist them in accounting for all classified material and equipment mailed or shipped from the unit/site.

1. Records of Return Receipt Cards. The OIC, CMCC will maintain returned record of receipt cards for two years. The reference does not require return receipt cards for Confidential material/equipment; however, because of the dispersal of the units within MARRESFOR, return receipt cards will be utilized for all classified material and equipment mailed or shipped from MARRESFOR Headquarters and subordinate units.

2. Tracer Action. If a return receipt card or any type of acknowledgment of receipt is not received after shipping or mailing classified material or equipment, the following tracer action will be initiated:

a. A letter identifying the material/equipment, classification and date mailed/shipped will be sent to the commanding officer of the activity if no reply has been received after 30 days.

b. A message will be sent if no reply is received after 60 days.

NOTE: If the response resulting from paragraphs 5002.2a indicates that the material has not been received, a postal or carrier tracer will be initiated and the Security Manager will be notified.

5003. HAND CARRYING CLASSIFIED MATERIAL AND EQUIPMENT. Individuals authorized to hand carry classified material or equipment must take every precaution to prevent the unauthorized

h. The classification of the contents is not denoted on the outer envelope or container.

i. The material is logged out in the unit outgoing log.

j. Secret material is sent via U.S. Postal Service Registered mail within and between the United States and its territories (except when size does not permit then see paragraph 15-3.6 of the reference). United States Postal Service (USPS) Express mail may also be used for the transmittal of Secret information within and between the 50 states, the District of Columbia, and the Commonwealth of Puerto Rico when time sensitive requirements must be met. USPS Express Mail is the only express mail service authorized for transmission of classified material. When using USPS Express Mail classified material must be prepared per paragraph 15-11 of the reference. Under no circumstances will the USPS Express Mail form 11-B "waiver of signature and indemnity" be executed, even for Confidential mail.

k. Secret material is sent via the Defense Courier Service (DEFCOS) to and from addressees outside the United States and its territories.

l. Confidential material is sent via U.S. Postal Service Registered mail to and from FPO and APO addressees.

m. NATO Confidential is sent via U.S. Postal Service Registered mail inside and outside the United States.

n. Confidential material is sent via U.S. Postal Service Certified or Registered mail to the State Department for forwarding by diplomatic pouch.

o. Confidential material is sent via U.S. Postal Service Certified mail to DOD contractors and non-DOD agencies of the Executive Branch.

p. Confidential material sent to Department of Defense activities is sent via U.S. Postal Service "First Class" or, if weighing over 12 ounces, via "PRIORITY MAIL" within and between the United States and its territories. The outer envelope or container is marked "Postmaster: Do Not Forward, Return to Sender". Express Mail may also be used for this category of material. See sub-paragraph (j) above for caveats.

2. Top Secret material will only be transmitted as outlined in paragraph 15-2 of the reference and only by:

a. The Defense Courier Service.

b. Cleared and designated U.S. military personnel or

SOP FOR ISP

CHAPTER 5

MAILING, HAND CARRYING, AND TRANSMISSION OF CLASSIFIED MATERIAL

5000. GENERAL. Chapter 15 of the reference sets forth the policies and procedures for transmission of classified material by the Department of the Navy. This chapter sets forth additional policies and procedures for the transmission of classified material for the MARRESFOR Headquarters, and subordinate units.

5001. PREPARATION OF CLASSIFIED MATERIAL FOR MAILING. The OIC, CMCC will be responsible for preparation and mailing of all classified material except for COMSEC and SCI material.

1. The OIC, CMCC will ensure the following is accomplished prior to mailing classified material.

a. The classified material is enclosed in two (2) opaque, sealed envelopes or containers of such strength and durability as to prevent items from breaking out of the container while in transit and to facilitate the detection of any tampering.

b. Classified written/typed material will be folded or packed so the text will not be in direct contact with the inner envelope or container.

c. The inner envelope or container shows the address of the receiving activity.

d. The inner envelope or container is properly marked with the highest classification of the contents enclosed.

e. A return receipt card (OPNAV Form 5511/10) is attached to the inner envelope/container. The receipt form will be unclassified and contain only the information necessary to identify the material. Once returned, the receipts will be retained for two years.

f. The inner and outer envelopes or containers are carefully sealed with brown paper sealing tape.

g. The outer envelope or container shows the complete and correct address of the command to receive the material and the return address. Addressing this envelope is the responsibility of the section requesting material to be mailed. Classified material will be addressed to an official Government activity or DOD contractor and not to an individual.

classified information that he/she was not eligible to receive;

4. At the end of a Limited Access Authorization.

3007. SECURITY AWARENESS. The Security Manager will establish procedures for the dissemination of current security information via signs, poster, bulletins, memorandums, electronic mail, or other means. Supervisors will ensure widest dissemination of security awareness information.

3008. CLASSIFIED MATERIAL CUSTODIAN TRAINING. The OIC, CMCC will provide appropriate security of classified information training to all CMCC and Secondary Control Point personnel upon their initial assignment to CMCC or SCP duties. Refresher training for these personnel will be conducted quarterly by the OIC, CMCC.

local Naval Criminal Investigative Service (NCIS) offices and can arrange for NCIS personnel to give this brief. Subordinate units that are not located near a NCIS office can request assistance from their higher headquarters.

3005. SPECIAL BRIEFINGS

1. Foreign Travel Brief. Any USMC, USN military or civilian who has had access to classified information and who plans to travel to or through one or more of the countries designated in exhibit 5A of the reference must be given a defensive briefing by the unit Security Manager prior to travel. It is the responsibility of the individual to notify the Security Manager prior to travel. This provision is applicable to official and unofficial travel. Reserve personnel who travel to these countries as a function of their civilian (non-government) job must also notify their military unit Security Manager.

2. Upon return to the United States personnel traveling to those designated countries will contact their unit Security Manager for debriefing.

3. Sensitive Compartmented Information (SCI) Brief. The Special Security Officer (SSO) will brief those individuals granted access to SCI.

4. NATO Brief. All personnel who require access to NATO information will be briefed by the OIC, CMCC or the NATO Sub Registry Control Officer on NATO security procedures.

5. Classified Material Courier Brief. Prior to issuing a courier card or classified material to a traveller authorized to hand carry classified material the OIC, CMCC will brief the individual on the proper responsibilities and procedures to be followed.

3006. DEBRIEFING. Personnel who have had access to classified information will be debriefed and appropriate security termination forms will be completed by the OIC, CMCC under the following circumstances:

1. Prior to termination of active military service or civilian employment;
2. When security clearance/access is revoked for cause or administratively withdrawn;
3. When the individual has inadvertently gained access to

briefings for all personnel granted access to classified material.

4. Section heads are responsible for ensuring that individuals under their control attend scheduled security education training. All sections that handle or process classified material will ensure that supplemental on the job training is given to their personnel.

3004. MINIMUM REQUIREMENTS

1. Indoctrination Brief. All personnel must have a basic understanding of what classified information is and why/how classified information is safeguarded. The Commanding Officer, Headquarters Battalion, MARRESFOR will ensure that all personnel reporting to the Headquarters MARRESFOR, 4th MarDiv, 4th MAW, and 4th FSSG receive an indoctrination brief that includes as a minimum those topics listed in paragraph 3-6.3 of the reference. The unit Site Commander has this responsibility for subordinate units.

2. Orientation Brief. Each person who requires access to classified information will receive an orientation brief from the OIC, CMCC prior to being granted access. The brief will be tailored to address the specific procedures and requirements within the unit.

3. On-the-Job-Training. Section heads will ensure that subordinates know the general security requirements and those security responsibilities specific to their individual duties. The primary responsibility of supervising on-the-job-training rests with the section head.

4. Refresher Training. The Headquarters Battalion, MARRESFOR training officer will schedule an annual security refresher brief for all personnel assigned to the Headquarters MARRESFOR, 4th MarDiv, 4th MAW, and 4th FSSG who have access to classified material. Unit training officers/NCO's have similar responsibility in subordinate units. The refresher training will be designed to reinforce security awareness and motivate security discipline. Changes in security policies and procedures, positive and negative trends noted in the command security program and special security considerations, such as the processing of classified information on computers, are examples of appropriate subjects. Command Security Managers are available to assist in developing this brief.

5. Counterespionage Briefing. Every two years, personnel with access to classified material will receive a counterespionage briefing. The Security Manager is authorized direct liaison with

SOP FOR ISP

CHAPTER 3

SECURITY EDUCATION

3000. BASIC POLICY. All personnel assigned to MARRESFOR and any subordinate unit are required to participate in the security education program. All personnel designated as a Security Manager, Assistant Security Manager, or Security Assistant will complete an approved course of instruction (resident or non resident) in Security Manager duties or in Security of Classified Information within six months of their appointment. The SNCOIC and all personnel working in the MARRESFOR CMCC will complete, as a minimum, the non resident Security Managers Course. All personnel who are responsible for or work with classified material on a daily basis are encouraged to complete the non resident Security Manager course in addition to the requirements listed below.

3001. PURPOSE. To ensure that all understand the need to protect and know how to safeguard classified information. The goal is to develop fundamental habits of security so that proper discretion and judgement will automatically be exercised in the discharge of duties involving classified information.

3002. SCOPE. Security education is required for all personnel without regard to their security clearance or access status. Those personnel with security clearances and access that work with classified material will be provided additional education and training.

3003. RESPONSIBILITY

1. The MARRESFOR Security Manager is responsible for overall policy guidance, establishing security education requirements, and coordinating support.

2. The MARRESFOR Headquarters Battalion training officer is responsible for scheduling and conducting security education briefs, as stated in paragraph 3004, below for personnel assigned to the Headquarters MARRESFOR, 4th MarDiv, 4th MAW, and 4th FSSG. The training officers/NCO's of subordinate units have a similar responsibility for their personnel. Appropriate training records documenting security education training will be maintained per current training directives.

3. The unit OIC, CMCC is responsible for conducting orientation

SOP FOR ISP

CHAPTER 5

MAILING, HAND CARRYING, AND TRANSMISSION OF CLASSIFIED MATERIAL

	PARAGRAPH	PAGE
GENERAL	5000	5-3
PREPARATION OF CLASSIFIED MATERIAL FOR MAILING	5001	5-3
RETURN RECEIPTS SYSTEM	5002	5-5
HAND CARRYING CLASSIFIED MATERIAL AND EQUIPMENT	5003	5-5
NAVAL MESSAGES	5004	5-7
FACSIMILE AND OTHER ELECTRONIC DATA . . .	5005	5-8
TELEPHONIC TRANSMISSIONS	5006	5-9

FIGURE

FORMAT FOR AUTHORIZATION TO HANDCARRY CLASSIFIED INFORMATION	5-1	5-10
SECURE FACSIMILE TRANSMISSION SHEET . . .	5-2	5-12

4015. FOREIGN TRAVEL

1. All personnel possessing a security clearance are required to report to their Security Manager all personal foreign travel in advance of the travel being performed. Personnel will be advised of the requirements to report such travel during the orientation briefing and annual refresher briefings.
2. The Security Manager will ensure that a foreign travel brief is conducted prior to personnel traveling abroad. It is recommended that the briefing be coordinated with the servicing NCIS office. A record will be kept of those personnel given the brief for a minimum of two years.
3. When the individual returns, they will be debriefed and provided the opportunity to report any incident, no matter how insignificant it might seem, that could have security implications.
4. When travel patterns (i.e., numerous expensive trips abroad or very frequent travel) or the failure to report such travel indicates the need for investigation, the matter will be referred to MARRESFOR.

4016. SUICIDE OR ATTEMPTED SUICIDE. If any person assigned to the MARRESFOR or subordinate unit who has access to classified material or equipment attempts to commit suicide, the Security Manager will immediately terminate the individual's access and forward all available information to the nearest NCIS office. The report will contain the nature and extent of the classified information to which the individual had access and the circumstances surrounding the attempted suicide. If the individual was a custodian and had access to classified material the combination must be changed and an inventory conducted immediately.

4017. UNAUTHORIZED ABSENTEES. When personnel of the MARRESFOR who have access to classified material and equipment are in an Unauthorized Absence (UA) status, the Security Manager will be notified. An inquiry will be conducted by the command to determine if there are any indications that the individual's activities, behavior or associations may be hostile to the interest of national security. If the individual in a UA status was a storage area custodian or had access to the security containers or storage area, an inventory will be conducted immediately. If the inquiry reveals indications that national security may be adversely affected, the servicing NCIS office will be immediately notified by the Security Manager.

immediately to their Security Manager. The Security Manager must notify the servicing NCIS office. If the local NCIS representatives are unavailable for assistance, the Security Manager may call the Navy Espionage Hot Line at 1-800-543-6289.

a. The MARRESFOR Security Manager will be contacted by the most expeditious means with details concerning the incident. All available information (who, what, where, and when) will be provided.

b. An immediate message with additional details will be sent to the Commanding General, MARRESFOR (Security Manager) within 24 hours of original telephonic notification.

2. The Security Manager will notify the servicing NCIS office immediately of any requests, through other than official channels, for classified national defense information or unclassified technical data with military or space applications. Examples of unclassified requests include: names, duties, personal data or characteristics of unit personnel, technical orders, technical manuals, regulations, military phone books, personnel rosters, unit manning tables, unit strength, mission, combat readiness, and development or effectiveness of weapon systems.

4014. CONTACT WITH CITIZENS OF DESIGNATED COUNTRIES

1. All personnel will promptly report to the Security Manager or Duty Officer any form of contact, intentional or unintentional, with any citizen, official, office, establishment or entity of a "designated country". A list of designated countries is contained in Exhibit 5A of the reference. The term contact means any form of encounter, association, or communication whether social, official, private or any other means.

2. Contacts with citizens of designated countries are not, in themselves, wrong, against regulations, or illegal. However, such contacts must be reported immediately to NCIS to permit NCIS to evaluate the contacts in order to protect the Department of the Navy from hostile intelligence activities. When personnel have contacts routinely or with great frequency, NCIS will advise such personnel as to any future reporting requirements. For example, an amateur radio operator may be in contact with citizens of designated countries on a regular basis. After receiving an initial report, NCIS will instruct the reporting individual on the conditions and requirements subsequent to reporting.

b. The Duty Officer will notify the Security Manager. The Security Manager will provide the Duty Officer additional guidance, as required.

c. The person discovering the open container will remain in the vicinity of the open security container or storage area door until the custodian arrives, if possible.

d. The custodian will conduct a complete inventory of the security container or storage area. A written report will be made to the Security Manager detailing any discrepancies or missing documents.

e. The person discovering the open container will prepare a written statement describing the circumstances leading to the discovery. The statement will be given to the Security Manager.

4010. UNSECURED MATERIAL. When an item of classified material is found unsecured (e.g., unattended on a desk, on the deck, in the trash), the finder will immediately bring it to the Security Manager or, if after working hours, to the Duty Officer. The Duty Officer will ensure that the material is properly safeguarded until the appropriate person responds to take custody of the material. A written report detailing the circumstances of the discovery and disposition of the material will be made to the Security Manager.

4011. IMPROPER TRANSMISSION OF CLASSIFIED MATERIAL. When an individual discovers that classified material or equipment has been improperly transmitted or damaged in shipment the individual will notify the Security Manager immediately. The Security Manager will forward a Security Discrepancy Notice, OPNAV Form 5511/51, to the sender of the material or equipment.

4012. COMMUNICATION SECURITY MATERIAL SYSTEM (CMS). When an individual discovers loss, physical compromise, or suspected compromise of Classified Communications Security (COMSEC) material, it will be reported to MARRESFOR Headquarters (Code G6/CMS) per appropriate CMS regulations. A preliminary inquiry will be conducted per paragraph 4004 above.

4013. SABOTAGE, ESPIONAGE, OR DELIBERATE COMPROMISE

1. Individuals becoming aware of possible acts of sabotage, espionage, deliberate compromise or terrorist activities will report all available information concerning such action

what, where, when, and why" questions concerning the security violation. Guidance for conducting a JAG Manual Investigation is contained in paragraph 4-5 of the reference. The investigating officer will consult with the Staff Judge Advocate before initiating a JAG Manual Investigation.

4006. INVESTIGATIVE ASSISTANCE. An Inquiry or JAG Manual Investigation Officer may require investigative assistance. If so, assistance may be provided by NCIS. Requests for NCIS investigative assistance will be coordinated through the Security Manager. Paragraph 4-6 of the reference pertains.

4007. COMPROMISE THROUGH PUBLIC MEDIA. Individuals becoming aware that classified information may have been compromised as a result of disclosure in the public media, (i.e., newspapers, books, radio or television broadcasts), will immediately notify the Security Manager. As many details as possible, such as the name of the reporter, newspaper, television show, dates, station, etc., should be provided. Local Security Managers will forward all such reports to the MARRESFOR Security Manager.

4008. OTHER SECURITY VIOLATIONS. Violations of security regulations which do not result in a compromise or subjection to compromise may be acted upon by the Commanding General without reporting to higher authority. However, if the circumstances of the security violation constitute a national security case, as determined by the Staff Judge Advocate, the case will be forwarded per the JAG Manual.

4009. UNSECURED CONTAINERS

1. A major security violation occurs when a container in which classified material is stored is found unsecured in the absence of assigned and cleared personnel. This includes open security containers in an unoccupied room with only a lock on the hatch to provide protection. Unless the room has been specifically approved for open storage this is a reportable security violation. If such an incident occurs during working hours, the Security Manager will be immediately notified.

2. If the incident occurs after normal working hours the Duty Officer will be notified immediately and the following steps will be taken:

a. The custodian(s) whose name is listed in the locking drawer of the security container, or on the inside of the storage area door, will be notified immediately.

SOP FOR ISP

CHAPTER 4

COMPROMISE AND SECURITY VIOLATION PROGRAM

4000. GENERAL. The compromise of classified information presents a threat to national security. The seriousness of that threat must be determined and measures taken to negate or minimize the adverse effects of the compromise. All security violations will be expeditiously reported, vigorously investigated, and corrective action taken to prevent a recurrence of the violation.

4001. SECURITY VIOLATIONS

1. There are two types of security violations:

a. Those that result in a confirmed or possible compromise of classified information, and;

b. Those that do not result in such a confirmed or possible compromise, but in which a security regulation has been violated.

2. Security violations of either type will be immediately reported via the most expeditious method to the Unit Security Manager then followed by a written report. The Unit Security Manager will initiate appropriate action per this Manual and chapter 4 of the reference.

3. Security violations will be vigorously investigated with the intent of identifying the security weakness or failure causing the violation. All findings must be documented and shall include recommendations for corrective action to ensure this violation will not occur again. This will be sent to the Commanding General, MARRESFOR (Security Manager) via the chain of command.

4. If the security violation occurred due to a failure to comply with the policies, procedures, and regulations for safeguarding classified information the investigation will contain a recommendation as to the continued security clearance/access eligibility of the individual committing the violation.

4002. ADMINISTRATIVE SANCTIONS, CIVIL REMEDIES, AND PUNITIVE ACTIONS

1. Civil employees are subject to administrative sanctions, civil remedies, and criminal penalties if they knowingly, willfully or negligently disclose classified information to an

unauthorized person or violate the provisions of the reference, this Manual, or other security regulations.

2. Military personnel are subject to punitive action, either in federal courts or under the Uniform Code of Military Justice, as well as administrative sanctions, if they disclose classified information to any unauthorized person, or violate the provision of the reference, this Manual, or other security regulation.

4003. DISCOVERY OF LOSS, COMPROMISE OR VIOLATION. Any individual who becomes aware of the loss, possible compromise or actual compromise of classified information or material will immediately notify the unit Security Manager. The Security Manager will notify the Commanding Officer and the nearest Naval Criminal Investigative Service (NCIS) field office.

4004. PRELIMINARY INQUIRY

1. When classified information has been lost, compromised or subjected to compromise, a preliminary inquiry will be conducted, after notification has been made to NCIS. The inquiry will be completed within 72 hours unless an extension has been granted by the MARRESFOR Security Manager.

2. The Commanding Officer will appoint an investigating officer to conduct the preliminary inquiry.

3. Every effort will be made to keep the inquiry unclassified. The fact that a compromise has occurred is not necessarily classified.

4. Specific guidelines for the conduct of a preliminary inquiry are contained in paragraph 4-4 of the reference. The preliminary inquiry officer will consult with the Staff Judge Advocate and Security Manager before initiating the inquiry.

5. If the inquiry determines that compromise is confirmed and that the probability of damage to national security cannot be discounted, significant activity weakness is revealed, or punitive action is appropriate, a JAG Manual Investigation will be initiated.

4005. JAG MANUAL INVESTIGATION. The JAG Manual Investigation is an administrative proceeding conducted per chapters II through IX of the Manual of the Staff Judge Advocate General. The purpose of the JAG Manual Investigation is to answer, in detail, "who,

SOP FOR ISP

CHAPTER 4

COMPROMISE AND SECURITY VIOLATIONS PROGRAM

	PARAGRAPH	PAGE
GENERAL	4000	4-3
SECURITY VIOLATIONS	4001	4-3
ADMINISTRATIVE SANCTIONS, CIVIL REMEDIES AND PUNITIVE ACTIONS	4002	4-3
DISCOVERY OF LOSS, COMPROMISE OR VIOLATION	4003	4-4
PRELIMINARY INQUIRY	4004	4-4
JAG MANUAL INVESTIGATION	4005	4-4
INVESTIGATIVE ASSISTANCE	4006	4-5
COMPROMISE THROUGH PUBLIC MEDIA	4007	4-5
OTHER SECURITY VIOLATIONS	4008	4-5
UNSECURED CONTAINERS	4009	4-5
UNSECURED MATERIAL	4010	4-6
IMPROPER TRANSMISSION OF CLASSIFIED MATERIAL	4011	4-6
COMMUNICATION SECURITY MATERIAL SYSTEM (CMS)	4012	4-6
SABOTAGE, ESPIONAGE, OR DELIBERATE COMPROMISE	4013	4-7
CONTACT WITH CITIZENS OF DESIGNATED COUNTRIES	4014	4-7
FOREIGN TRAVEL	4015	4-8
SUICIDE OR ATTEMPTED SUICIDE	4016	4-8
UNAUTHORIZED ABSENTEES	4017	4-8

SOP FOR ISP

CHAPTER 3

SECURITY EDUCATION

	PARAGRAPH	PAGE
BASIC POLICY	3000	3-3
PURPOSE	3001	3-3
SCOPE	3002	3-3
RESPONSIBILITY	3003	3-3
MINIMUM REQUIREMENTS	3004	3-4
SPECIAL BRIEFINGS	3005	3-5
DEBRIEFING	3006	3-5
SECURITY AWARENESS	3007	3-6
CLASSIFIED MATERIAL CUSTODIAN TRAINING .	3008	3-6

SOP FOR ISP

HEADING

[10]

CMS 4L

(date): _____

From: _____
 To: Director, Communications Security Material System
 Subject: LETTER OF APPOINTMENT

Ref: (a) CMS 4L Article 101
 (b) CSP 1A

1. The following personnel are appointed as CMS custodian and alternates for this command in accordance with reference (a):

a. CMS account number: _____ Phone numbers: AV _____ COMM _____

b. CMS account custodian: _____
 Grade and SSN: _____ Security clearance: _____
 Date of appointment: _____
 Date completed CMS Custodian Course (A-4C-0014): _____
 Name/location of CMS school attended: _____
 Sample signature: _____

c. Primary alternate custodian: _____
 Grade and SSN: _____ Security clearance: _____
 Date of appointment: _____
 Date completed CMS Custodian Course (A-4C-0014): _____
 Name/location of CMS school attended: _____
 Sample signature: _____

d. Second alternate custodian: _____
 Grade and SSN: _____ Security clearance: _____
 Date of appointment: _____
 Date completed CMS Custodian Course (A-4C-0014): _____
 Name/location of CMS school attended: _____
 Sample signature: _____

e. Third alternate custodian: _____
 Grade and SSN: _____ Security clearance: _____
 Date of appointment: _____
 Date completed CMS Custodian Course (A-4C-0014): _____
 Name/location of CMS school attended: _____
 Sample signature: _____

2. Two-person integrity required by reference (b) is in effect: Yes _____ No _____
 (If "No" include reason for non-compliance.)

3. Was a waiver of custodian/alternate custodian appointment criteria in reference (b) required? Yes _____ No _____ (If "Yes" include copy of approved waiver.)

4. Was a waiver to appoint less or more than the three alternate custodians required by reference (b) required? Yes _____ No _____ (If "Yes" include copy of approved waiver.)

5. If waiver to appoint more than three alternate custodians was obtained, list additional alternate custodians on reverse side in same format as paragraph 1 above.

Figure 2-9.--Format for Appointment of CMS Custodian.

SOP FOR ISP

HEADING

5510
(Section)
Date

From: Assistant Chief of Staff, G-6
(or Unit Commander)
To: (Rank, Name, SSN of Appointee)
Subj: APPOINTMENT AS ADP SECURITY OFFICER

Ref: (a) MCO P5501.14
(b) TASO Users Manual for TSS/NSS of May 1985
(c) Computer Access Device and Computer Fraud and Abuse
Act of 1984
(d) OPNAVINST 5510.1_
(e) ForO P5510.1

1. Per the references, you are hereby appointed as the ADP Security Officer, MARRESFOR (or unit) vice (Rank, Name, SSN of previous appointee), who stands relieved.

2. You are directed to become familiar with the references and all other pertinent or applicable directives or instructions pertaining to this appointment.

Signature

Copy to:
Security Manager

FIRST ENDORSEMENT

From: (Rank, Name, SSN of Appointee)
To: Assistant Chief of Staff, G-6

1. I have familiarized myself with the references and have assumed the duties as the ADP Security Officer for (unit).

Signature

SOP FOR ISP

HEADING

5510
(Section)
Date

From: MARRESFOR Top Secret Control Officer
To: (Rank, Name, SSN of Appointee)

Subj: APPOINTMENT AS TOP SECRET CONTROL ASSISTANT

Ref: (a) ForO P5510.1
(b) OPNAVINST 5510.1_

1. Per the references, you are hereby appointed as the Top Secret Control Assistant, MARRESFOR vice (Rank, Name, SSN of previous appointee), relieved.
2. You are directed to become familiar with the references and all other pertinent or applicable directives or instructions pertaining to this appointment.

Signature

Copy to:
MARRESFOR Security Manager

FIRST ENDORSEMENT

From: (Rank, Name, SSN of Appointee)
To: Top Secret Control Officer

1. I have familiarized myself with the references and have assumed the duties of Top Secret Control Assistant.

Signature

SOP FOR ISP

HEADING

5510
(Section)
Date

From: Adjutant
To: (Rank, Name, SSN of Appointee)
Subj: APPOINTMENT AS COSMIC CONTROL OFFICER
Ref: (a) ForO P5510.1
(b) OPNAVINST C-5510.101_

1. Per the references, you are hereby appointed as the COSMIC Control Officer, MARRESFOR vice (Rank, Name, SSN of previous appointee), who stands relieved.
2. You are directed to become familiar with the references and all other pertinent or applicable directives or instructions pertaining to this appointment.
3. You are directed to conduct a joint inventory of the classified material or other accountable material in custody and report in writing the results to the MARRESFOR Security Manager no later than (date).

Signature

Copy to:
MARRESFOR Security Manager

FIRST ENDORSEMENT

From: (Rank, Name, SSN of Appointee)
To: MARRESFOR Adjutant

1. I have familiarized myself with the references and have assumed the duties of COSMIC Control Officer, MARRESFOR. An inventory will be submitted as directed.

Signature

SOP FOR ISP

HEADING

5510
(Section)
Date

From: Adjutant
To: (Rank, Name, SSN of Appointee)
Subj: APPOINTMENT AS TOP SECRET CONTROL OFFICER (TSCO)
Ref: (a) ForO P5510.1
(b) OPNAVINST 5510.1_

1. Per the references, you are hereby appointed as the Top Secret Control Officer vice (Rank, Name, SSN of previous appointee), who stands relieved.
2. You are directed to become familiar with the references and all other pertinent or applicable directives or instructions pertaining to this appointment.
3. You are directed to conduct a joint inventory of the classified material or other accountable material in custody and report in writing the results to the Security Manager no later than (date).

Signature

Copy to:
MARRESFOR Security Manager
MARRESFOR Adjutant

FIRST ENDORSEMENT

From: (Rank, Name, SSN of Appointee)
To: Adjutant

1. I have familiarized myself with the references and have assumed the duties of Top Secret Control Officer, MARRESFOR. An inventory will be submitted as directed.

Signature

Figure 2-5.--Format for Appointment of Top Secret Control Officer.

SOP FOR ISP

HEADING

5510
(Section)
Date

From: (Section Head, Appropriate Section Identifier)
To: (Rank, Name, SSN of Appointee)

Subj: APPOINTMENT AS THE SECONDARY (or SUB-CUSTODY) CONTROL POINT
CUSTODIAN FOR (SECTION)

Ref: (a) ForO P5510.1
(b) OPNAVINST 5510.1
(c) (Unit Security Sop)

1. Per the references, you are hereby appointed as the Secondary (Sub-custody) Control Point Custodian for (Section) vice (Rank, Name, SSN of previous appointee), who stands relieved.
2. You are directed to become familiar with the references and all other pertinent or applicable directives or instructions pertaining to this appointment.
3. You are directed to conduct a joint inventory of the classified material or other accountable material in custody and report the results to the (Section Head) in writing no later than (date).

Signature

Copy to:
Unit Security Manager
OIC, CMCC

FIRST ENDORSEMENT

From: (Rank, Name, SSN of Appointee)
To: (Section Head, Appropriate Section Identifier)

1. I have familiarized myself with the references and have assumed the duties of Secondary (Sub-custody) Control Point Custodian for (Section). An inventory will be submitted as directed.

Signature

Figure 2-4.--Format for Appointment of Secondary/Sub-Custody Control Point Custodian.

SOP FOR ISP

HEADING

5510
(Section)
Date

From: MARRESFOR Adjutant or Unit Site Commander
To: (Rank, Name, SSN of Appointee)

Subj: APPOINTMENT AS OFFICER IN CHARGE, CLASSIFIED MATERIAL CONTROL
CENTER (OIC, CMCC)

Ref: (a) OPNAVINST 5510.1_
(b) ForO P5510.1

1. Per the references, you are hereby appointed as the Officer in Charge, Classified Material Control Center, vice (Rank, Name, SSN SSN of previous appointee), who stands relieved.
2. You are directed to become familiar with the references and all other pertinent or applicable directives or instructions pertaining to this appointment.
3. You are directed to conduct a joint inventory of the classified material or other accountable material in custody and report in writing the results to the Security Manager no later than (date).

Signature

Copy to:
Unit Security Manager

FIRST ENDORSEMENT

From: (Rank, Name, SSN of Appointee)
To: Same person/title listed on From section above

1. I have familiarized myself with the references and have assumed the duties of OIC, CMCC. An inventory will be submitted as directed.

Signature

Figure 2-3.--Format for Appointment of Officer in Charge, Classified
Material Control Center.

SOP FOR ISP

HEADING

5510
(SECTION)
Date

From: Commanding General (Unit Site Commander)
To: (Rank, Name, SSN of Appointee)

Subj: APPOINTMENT OF (UNIT) SECURITY MANAGER (or UNIT ASSISTANT
SECURITY MANAGER)

Ref: (a) ForO P5510.1
(b) OPNAVINST 5510.1_
(c) (Unit SecSop)

1. Per the references you are hereby appointed as the (unit)
Security Manager (or Assistant Security Manager) vice (Rank, Name,
SSN of previous appointee), who stands relieved.

2. You are directed to become familiar with the references,
and all other pertinent or applicable directives or instructions
pertaining to this appointment.

Signature

Copy to:
Adjutant
OIC, CMCC

FIRST ENDORSEMENT

From: (Rank, Name, SSN of Appointee)
To: (Same as from section above)

Subj: APPOINTMENT OF (UNIT) SECURITY MANAGER (or ASSISTANT SECURITY
MANAGER)

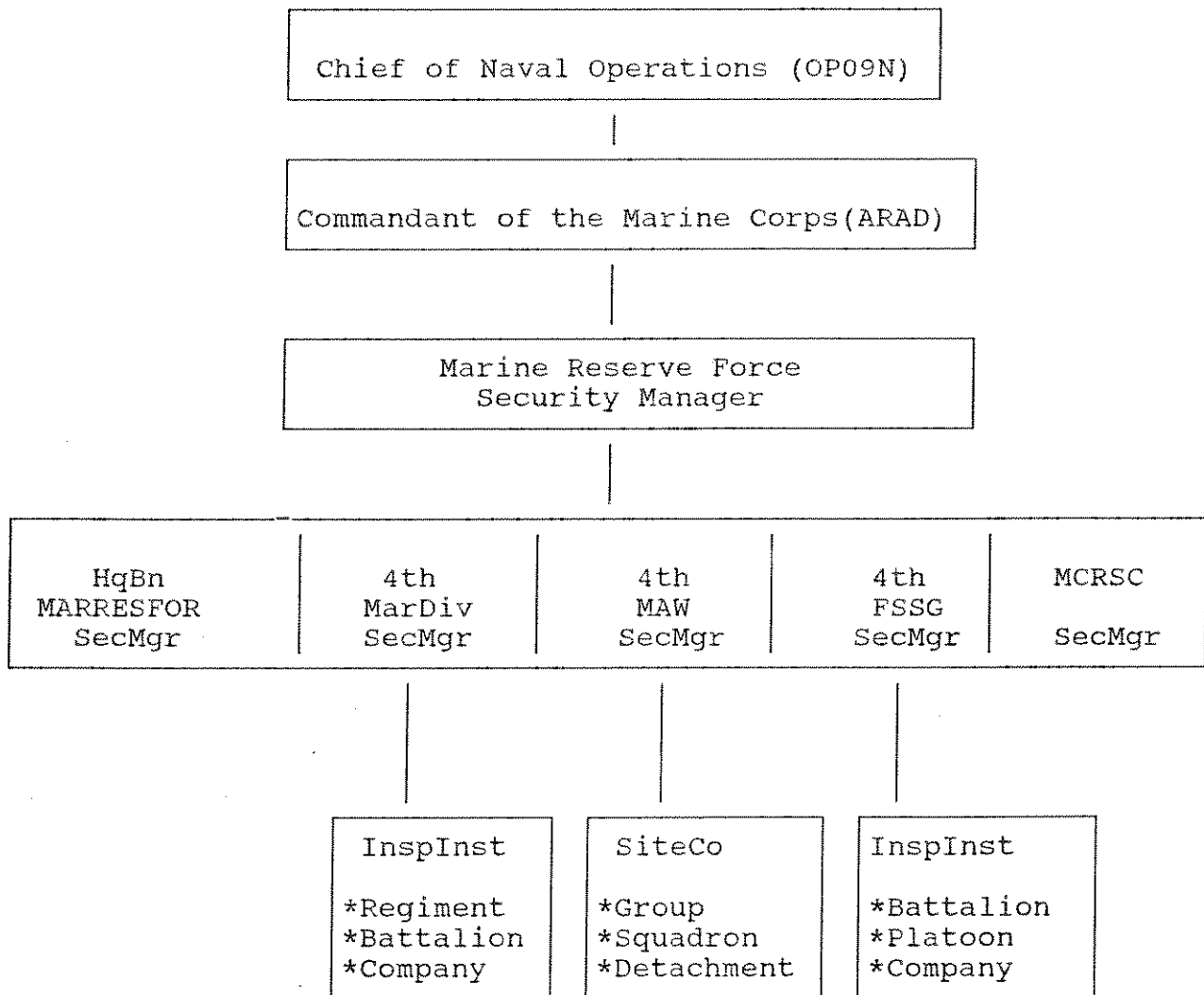
1. I have familiarized myself with the references and have assumed
the duties of Security Manager (or Assistant Security Manager).

Signature

Figure 2-2.--Format for Appointment of Security Manager/Assistant
Security Manager.

SOP FOR ISP

ORGANIZATIONAL STRUCTURE



(* = when mobilized)

Figure 2-1.--Organizational Structure.

2007. LETTERS OF APPOINTMENT. As indicated in paragraph 2001 above, the following Information and Personnel Security Program positions require written designation. Figures 2-2 through 2-9 are sample letters.

1. MARRESFOR (Unit) Security Manager.
2. Assistant Security Manager.
3. Headquarters Battalion Security Manager.
4. Officer in Charge, CMCC.
5. Secondary Control Point Custodian (SCPC), Alternate Secondary Control Point Custodian (AltSCPC).
6. Sub-Custody Control Point (SCCP) Custodian.
7. Top Secret Control Officer (TSCO) / Critical Nuclear Weapons Design Information (CNWDI) Custodian.
8. Top Secret Control Assistant (TSCA).
9. ADP Security Officer.
10. CMS Custodian (Primary and All Alternates).
11. Sealed Authentication System (SAS) Custodian.
12. NATO Sub-registry Control Point Officer.
13. Special Category Material (SPECAT) Focal Point Control Officer.
14. Special Security Officer (SSO).

b. The Staff Duty Officer or Staff Duty NCO will accompany the inspectors.

c. During the inspection, command duty personnel will open locked working spaces upon request of the inspector. If keys (or combinations) to these spaces are not available to them, duty personnel will recall the appropriate personnel to open them, at the discretion of the senior inspector.

d. All work areas may be subject to inspection with the exception of CMS and SCIF areas which are specifically excluded from USI's.

e. If classified material is found unsecured by the inspectors, the individual responsible for the material (CMCC/SCPO) will be notified by the SDO to report and secure the material. If appropriate, an inventory will be immediately initiated.

f. Command duty personnel will log in the identities of the inspectors, the time the inspection began and ended, and the results of the inspection.

g. The senior inspector will forward a written report of the inspection results to the MARRESFOR Chief of Staff, appropriate Security Manager, cognizant Staff Section, and the Unit Commander within five working days.

2004. TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM). TSCM surveys and inspections are performed upon request only in areas where highly classified information is regularly discussed. Requests for TSCM services will be addressed to the MARRESFOR Security Manager in writing and will be classified at least Secret. TSCM services will not be requested by telephone or other means. Discussions regarding these services will not be conducted in the area to be serviced and will be limited to those personnel with a valid "need to know".

2005. EMERGENCY PLANS. The Security Manager will ensure that the OIC, CMCC, COMSEC Officer, and the SSO develop a fully coordinated Emergency Action Plan for the protection of classified material in case of natural disaster, civil disturbance or enemy action. Emergency Action Plans will be published by each subordinate unit and tested for viability annually.

2006. FORMS. The reference lists the forms used in the Information and Personnel Security Program. Each chapter of this Manual lists forms and figures used by MARRESFOR.